

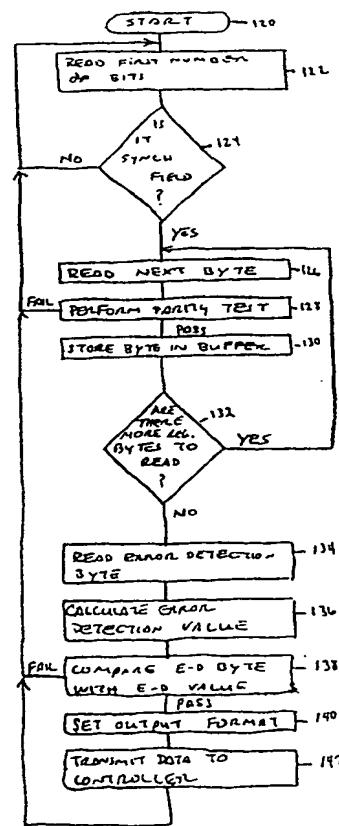


## INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification <sup>7</sup> :	A2	(11) International Publication Number:	<b>WO 00/11592</b>
G06K 7/00		(43) International Publication Date:	2 March 2000 (02.03.00)
(21) International Application Number:	PCT/US99/18691		
(22) International Filing Date:	17 August 1999 (17.08.99)		
(30) Priority Data:	09/138,589                    21 August 1998 (21.08.98)                    US		
(71) Applicant:	KERI SYSTEMS, INCORPORATED [US/US]; Suite 100, 1530 Old Oakland Road, San Jose, CA 95112 (US).		
(72) Inventors:	GEISZLER, Kenneth, J.; 182 Del Prado, Campbell, CA 95008 (US). WALKER, Russel, E.; 4271 North First Street #13, San Jose, CA 95134 (US). WHISTON, Kenneth, Alan; 141 Reed Way, Santa Cruz, CA 95060 (US). KWONG, Jon; 3254 Knight Wood Way, San Jose, CA 95148 (US). LINDSETH, Dale; 138 Pan Tempo Way, Hollister, CA 95023 (US).		
(74) Agents:	D'ALESSANDRO, Kenneth et al.; D'Alessandro & Ritchie, P.O. Box 640640, San Jose, CA 95164-0640 (US).		
(54) Title:	RADIO FREQUENCY IDENTIFICATION SYSTEM		

## (57) Abstract

A radio frequency identification system includes a transponder and a transponder reader. The transponder, responsive to an interrogation signal continuously transmitted by the transponder reader, generates a transponder signal modulated by an identification signal readable by the transponder reader. The identification signal includes a synchronization portion, a data portion, an output format identification portion, and an error detection portion. The output format identification portion is used by the reader to configure itself for communication with an attached controller. In another aspect of the invention, the transponder reader may be configured to read FSK as well as PSK encoded signals from the transponder.



**FOR THE PURPOSES OF INFORMATION ONLY**

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece	ML	Mali	TR	Turkey
BG	Bulgaria	HU	Hungary	MN	Mongolia	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MR	Mauritania	UA	Ukraine
BR	Brazil	IL	Israel	MW	Malawi	UG	Uganda
BY	Belarus	IS	Iceland	MX	Mexico	US	United States of America
CA	Canada	IT	Italy	NE	Niger	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NL	Netherlands	VN	Viet Nam
CG	Congo	KE	Kenya	NO	Norway	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NZ	New Zealand	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	PL	Poland		
CM	Cameroon	KR	Republic of Korea	PT	Portugal		
CN	China	KZ	Kazakhstan	RO	Romania		
CU	Cuba	LC	Saint Lucia	RU	Russian Federation		
CZ	Czech Republic	LI	Liechtenstein	SD	Sudan		
DE	Germany	LK	Sri Lanka	SE	Sweden		
DK	Denmark	LR	Liberia	SG	Singapore		
EE	Estonia						

## SPECIFICATION

### TITLE OF THE INVENTION

### RADIO FREQUENCY IDENTIFICATION SYSTEM

5

### BACKGROUND OF THE INVENTION

#### 1. Field of the Invention

This invention is directed generally to the field of radio frequency RF identification systems employing an electronic transponder and a transponder reader which emits an RF interrogation signal at a first frequency which powers the electronic transponder and enables it 10 to transmit a response on a second frequency (usually a lower frequency). Such systems are used in a number of fields including access security, object identification, inventory control, and generally any field where a small transponder unit may be associated with an object and remotely probed and read by a radio frequency transmission emitted by a transponder reader.

#### 2. The Background Art

15 Radio frequency identification systems are well known in the art. Such systems are commonly in use in building access schemes where an authorized user of the building is given a building access card containing an authorization code number stored and optionally encrypted on the card as a binary string of data. The card is then presented to a transponder reader which continuously transmits an RF interrogation signal. The card containing a 20 transponder receives the continuously transmitted signal from the transponder reader, uses it to power circuitry on board the card, modulate an RF carrier signal having a different frequency (usually lower) from that of the RF interrogation signal received from the reader (typically an integer fraction of the RF interrogation signal frequency, e.g., 1/2, 1/3, 1/4, etc.) with an identification signal stored on the transponder and containing an authorization code number, 25 and the transponder reader then reads the identification signal emitted from the transponder and passes the authorization code number to an appropriate controller for determining whether or not the authorization code number received is sufficient to allow the user access to the building. If the authorization code number is sufficient, generally a lock will be opened enabling a door to be opened and optionally a computer will log the entry for future reference.

30

Other implementations of such systems enable object identification by reading a

transponder attached to or embedded in the object (e.g., cargo identification, pet identification, taxi identification at an airport, and the like).

Generally, all existing transponder readers of such radio frequency identification systems utilize proprietary systems. That is, a card from one system will not be readable by a system provided by another vendor. In some systems, the transponder emits a signal modulated by frequency shift keying (FSK), i.e., the binary transmission is represented by a mark and a space which correspond to the 1 and 0 of the binary signal, the mark and space being signals on two separate frequencies (e.g., 1/8 and 1/10 of the frequency of the RF interrogation signal). Other systems utilize phase shift keying (PSK) as well known in the art.

5 Systems using PSK modulation cannot read the cards which transmit FSK modulated information and systems which read FSK modulated information cannot read the cards which transmit PSK modulated information.

10

While all such transponder readers read matching transponder cards, in most systems they are also required to communicate with a controller of some sort. The controller generally comprises a central processing unit (CPU) which may interact with a number of such readers which are simultaneously connected to it. A number of different systems have evolved over the years for communicating data from a reader to a controller. Some of these systems, or communications protocols, are known as magnetic stripe communications protocol, Wiegand communications protocol, single wire Wiegand communications protocol, RS232 communications protocol, RS422 communications protocol, and the like. These various communication protocols generally require 1, 2, 3 or more electrical wire connections between the transponder reader and the controller. Furthermore, the data modulation schemes for these various systems differ as well known to those of ordinary skill in the art. This has led to a problem in the industry in the stocking of transponder readers. In order to stock transponder readers which are compatible with the various communications protocols employed by the various controllers, one needs to stock many transponder readers which are mutually incompatible with one another. A need, therefore, exists for a transponder reader which is capable of working with a number of different communication protocols in communicating with a corresponding controller so as to reduce the inventory requirements for transponder readers.

15

20

25

30

It is also desirable to have the transponder reader require as little field programming as possible. In this way, relatively unskilled personnel may successfully install transponder readers and have them operate with corresponding controllers and transponders with relatively little difficulty. To avoid the necessity to physically program such readers to communicate

using a given communications protocol (as by setting DIP switches or jumpers) would be highly desirable.

#### OBJECTS AND ADVANTAGES OF THE INVENTION

Accordingly, it is an object and advantage of the present invention to provide an  
5 improved RF identification system.

It is a further object and advantage of the present invention to provide an improved transponder reader for use in RF identification systems.

It is a further object and advantage of the present invention to provide a capability to  
10 program the transponder reader to communicate with an attached controller using a communications protocol specified by information contained in an output format identification portion of the identification signal stored in the transponder and transmitted to the transponder reader.

It is a further object and advantage of the present invention to provide an improved  
15 transponder for use in an RF identification system.

It is a further object and advantage of the present invention to provide a transponder for  
use in an RF identification system which contains an identification signal which has within it,  
in addition to an authorization code number, an output format identification portion which,  
when transmitted to and received by the transponder reader, defines the communications  
20 protocol to be used by the transponder reader in communicating with attached devices such as a controller.

Yet another object and advantage of the present invention is the provision of a transponder reader capable of reading both PSK and FSK signals.

Yet another object and advantage of the present invention is the provision of a  
25 mechanism by which either the PSK or the FSK mode of operation may be normally disabled  
and easily authorized in an accountable manner.

These and many other objects and advantages of the present invention will become apparent to those of ordinary skill in the art from a consideration of the drawings and ensuing description of the invention.

## SUMMARY OF THE INVENTION

A radio frequency identification system includes a transponder and a transponder reader. The transponder, responsive to an interrogation signal continuously transmitted by the transponder reader, generates a transponder signal modulated by an identification signal readable by the transponder reader. The identification signal includes a synchronization portion, a data portion, an output format identification portion, and an error detection portion. The output format identification portion is used by the reader to configure itself for communication with an attached controller. In another aspect of the invention, the transponder reader may be configured to read FSK as well as PSK encoded signals from the transponder.

## BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a system block diagram of an RF identification system in accordance with a presently preferred embodiment of the present invention.

FIG. 2 is a sectional top plan view of a transponder card in accordance with a presently preferred embodiment of the present invention.

FIG. 3 is a detailed system block diagram of an RF identification system in accordance with a presently preferred embodiment of the present invention.

FIG. 4 is a timing and data output diagram for a conventional Wiegand output data stream.

FIG. 5 is a timing and data output diagram for a conventional mag stripe output data stream.

FIG. 6 is a block diagram of a circuit for receiving transponder signals modulated with either PSK or FSK modulation techniques in accordance with a presently preferred embodiment of the present invention.

FIG. 7 is a detailed circuit diagram for circuit for receiving transponder signals modulated with either PSK or FSK modulation techniques in accordance with a presently

preferred embodiment of the present invention.

FIG. 8 is a diagram showing the layout of data stored on a transponder card in accordance with a presently preferred embodiment of the present invention.

5 FIG. 9 is a flow chart diagraming a method for reading and verifying data received from a transponder card in accordance with a presently preferred embodiment of the present invention.

10 FIG. 10 is a partial block diagram of a modification of the circuit of FIG. 6 in which programmable switches control the flow of RF signal through the PSK and FSK signal processing branches of the transponder reader in accordance with a presently preferred embodiment of the present invention.

#### DESCRIPTION OF THE PREFERRED EMBODIMENTS

Those of ordinary skill in the art will realize that the following description of the present invention is illustrative only and is not intended to be in any way limiting. Other 15 embodiments of the invention will readily suggest themselves to such skilled persons from an examination of the within disclosure.

The present invention is directed to a radio frequency (RF) identification system which solves many problems of the prior art. Turning now to Fig. 1, a system diagram of a radio frequency identification system generally denoted 10 in accordance with a presently preferred embodiment of the present invention is shown. System 10 includes a transponder reader 12, a controller 14, and something controlled by the controller such as a door lock 16, and a transponder 18. As with all such radio frequency identification systems, transponder reader 12 preferably continuously emits a radio frequency interrogation signal of a given frequency. According to presently preferred embodiments of the present invention, the interrogation 20 signal is either at approximately 125 KHz or at approximately 13.56 MHz although those of ordinary skill in the art will realize that virtually any other frequency in the RF spectrum could be used. The radio frequency signal is received by transponder 18 which includes an antenna and a rectifier circuit or "power circuit" for deriving electrical power from the received signal. Transponder 18 then transmits, in response to receipt of the interrogation signal from 25 transponder reader 12, a transponder signal of a lower frequency than the interrogation signal having modulated thereon a stored identification signal in the form of a binary data stream. As long as the transponder 18 is close enough to transponder reader 12 that it can receive the 30

interrogation signal therefrom, it will also continuously transmit a transponder signal which can then be picked up by the transponder reader 12 and demodulated.

Upon demodulating the transponder signal, transponder reader 12 obtains therefrom the identification signal originally stored on card 18. A portion of the identification signal is an authorization code number. That authorization code number is passed from transponder reader 12 to controller 14 over data communication line 20 in accordance with a given data communications protocol. In accordance with a presently preferred embodiment of the present invention, the data communications protocol used over line 20 is specified by an output format identification portion of the identification signal transmitted from transponder 18 to transponder reader 12. The protocol may be preferably one of several well known in the art such as, for example, RS232, RS422, various versions of the Wiegand protocol, and various versions of the mag stripe protocol. Other protocols may also be specified and used where appropriate.

The ability to store the selected data communications protocol to be used by a transponder reader 12 reading the transponder at the time of initially programming the transponder 18 permits a single transponder reader 12 to be used with a variety of controllers 14 and avoids the necessity for stocking a number of different transponder readers each compatible with a particular controller system.

Upon receipt of a valid authorization code number over line 20, controller 14 then activates door lock 16 or other appropriate apparatus as well known to those of ordinary skill in the art.

Turning now to FIG. 2, a top view of a typical transponder 18 is shown. Transponder 18 comprises an antenna 22 connected to a transponder integrated circuit 24 all preferably embedded within a plastic card or tag 26 or otherwise encapsulated. According to a presently preferred embodiment of the present invention, the integrated circuit is a Micro Chip Technology MCRF250 or MCRF350. The MCRF250 operates at 125 KHz and the MCRF350 operates at 13.56 MHz. Those of ordinary skill in the art will realize that this particular integrated circuit can be substituted for individual components or other integrated circuits made by other manufacturers in order to achieve the same purpose and function. Micro Chip Technology, Inc. is located in Chandler, Arizona and on the World Wide Web at [www.microchip.com](http://www.microchip.com).

Turning now to FIG. 3, a detailed block diagram of a system in accordance with the present invention is shown. Reader or transponder reader 12 includes an RF transmitter section 28 which generates an RF carrier signal which is coupled to antenna 30 for transmission from reader transponder 12. Also coupled to antenna 30 is an RF receiver section for receiving and demodulating signals received from the transponder 18 over antenna 30. Coupled to the RF receiver section is a CPU 32 which processes and demodulates the identification signal received from the transponder 18 and sets the communications protocol to be used in communicating between transponder reader 12 and controller 14 in accordance with an output format identification portion of the identification signal received from the transponder module 18. CPU 32 is coupled to conventional output drivers 34 and a data link 36 communicating with controller 14.

Controller 14 includes typical input circuitry 38 coupled to a conventional CPU 40 which is in turn coupled to programmable memory 42 for storing access criteria to be compared with the authorization code number received from the transponder reader 12. CPU 40 is also coupled to driver circuitry 44 of a conventional nature for driving a door lock or other associated apparatus 16 upon determination by CPU 40 that access is permitted. Those of ordinary skill in the art will also realize that this system can easily be adapted to systems for inventory control and object identification and tracking, e.g., by recording the presence of a serial number received from a transponder module rather than by opening a door lock.

Transponder 18 comprises an antenna 46 coupled to a power circuit 48 which rectifies a received interrogation signal from transponder reader 12 to power the circuitry of transponder 18. Also coupled to antenna 46 is a frequency divider circuit 50 for providing a carrier signal to transmitter 52 (also coupled to antenna 46). Frequency divider 50 provides a signal used by transmitter 52 to modulate an identification signal onto. The identification signal is preferably stored as a binary 128 bit value in memory 54. Those of ordinary skill in the art will realize that other numbers of bits could be used as could non-binary values. Memory 54 is preferably a one time programmable memory cell, such as an EEPROM. Upon activation by the presence of an interrogation signal, transmitter 52 transmits an identification signal modulated onto a carrier at an integer fraction of the interrogation signal. For a 125 KHz system (i.e., one operating with an interrogation signal of 125 KHz), the transponder signal in PSK mode is at approximately 62.5 KHz and in FSK mode is at 12.5 KHz and 15.625 KHz for the mark and space (the one that is the mark and the one that is the space are a matter of choice for the developer).

Turning now to FIG. 4, the output of a Wiegand output stream is depicted. In the

Wiegand output protocol there are two active lines, one associated with the binary value 1 and the other associated with the binary value 0. To indicate the presence of a 1, the 1 line goes high and the 0 line stays low. To indicate the value of 0, the 0 line goes high and the 1 line stays low. FIG. 4 indicates the manner in which the binary value 10110 would be transmitted over this pair of lines.

FIG. 5 shows data transmission in accordance with the conventional mag stripe output protocol. In the mag stripe protocol, there are two lines for conveying data, one is a clock line (CLK) and one is a data line (DATA). The clock line generates a pulse at a regular time interval. The data line generates a pulse corresponding with a clock pulse to represent a 1 and the lack of a pulse corresponding with a clock pulse indicates a 0. The signals shown in FIG. 5 indicate how the binary value 1011101 would be transmitted over this pair of lines in a conventional mag stripe output protocol.

Those of ordinary skill in the art will realize that there are a number of different ways to transmit such data including RS422, RS232, various versions of the mag stripe output stream format including open collector versions thereof and various versions of the Wiegand output stream format including open collector versions thereof and single wire versions thereof. The advantage of this aspect of the present invention is that the transponder reader 12 can be simply programmed by the transponder to output data to the controller 14 in any one of a number of different data communications protocols by simply setting the output format identification portion of the identification signal stored on the transponder 18 to the correct value corresponding to that particular communications protocol.

In practice, an installer would purchase a transponder reader 12 in accordance with the present invention and connect it to an existing controller 14 having a given data communications protocol. The transponders 18 would then all be programmed in accordance with the controller's requirements. A data communications protocol would be specified in the output format identification portion of the identification signal stored on the transponder 18 (this value is not passed to the controller 14). Where the card is read, the reader automatically passes only the authorization code number to the controller 14 in accordance with the specified protocol.

Turning now to FIG. 6, an additional aspect of the invention is disclosed. Because most transponders used in RF identification systems use either phase shift keying (PSK) or frequency shift keying (FSK), it has usually been the case that transponders and transponder readers had to comport with one standard or the other standard, i.e., PSK or FSK. No prior

known systems are capable of dual mode operation. In accordance with the present invention, however, the front end of the reader comprises two distinct signal processing paths. The first path processes PSK signals and the second path processes FSK signals. Generally, PSK signals are at a carrier frequency of one-half (or another integer fraction) of the interrogation signal frequency. That means, for an interrogation signal frequency of 125 KHz, the transponder's response PSK signal would be at 62.5 KHz. FSK signals, on the other hand, commonly have a mark signal and a space signal, one of the mark and space signals being at one-eighth the interrogation signal frequency and the other being at one-tenth the interrogation signal frequency. Other frequency shifts may be used. Thus, an FSK signal might have a mark at 12.5 KHz, and a space at 15.625 KHz, or vice versa. It is therefore possible, with filters, to direct the two signal trains through different branches of a circuit for processing.

Turning now to FIG. 6, an antenna 70 associated with the transponder reader 12 receives a signal from transponder 18 and passes it to circuit node 72. At circuit node 72, the signal will pass along branch 74 if it is a PSK signal, i.e., it has a first frequency less than the frequency of the interrogation signal. Similarly, the signal will pass along branch 76 for FSK processing if it has a frequency less than that of a PSK signal. In this example, assuming that the interrogation signal is a 125 KHz signal, 62.5 KHz signals will pass along the PSK branch 74 and 12-15 KHz signals will pass along the FSK branch 76. This is made possible by the use of filters. Filter No. 1 (78) is designed to pass frequencies consistent with the PSK signal pass band. In this example, those frequencies would be near 62.5 KHz. Filter 78 is designed to reject frequencies at 125 KHz as well as to reject frequencies significantly below 62.5 KHz, such as a FSK signals at 12-16 KHz. Turning to the FSK processing branch 76, discriminator 80 is used in a conventional manner to discriminate or AM envelope detect the mark and space FSK signals at 12-16 KHz. Filter No. 2 (82) is designed to stop 125 KHz signals but to pass those signals in the range of 12-16 KHz. The PSK and FSK branches 74 and 76 rejoin at node 1 (84) and are then passed through filter no. 3 (86) which also rejects 125 KHz signals whereupon they reach node 2 (88) and are input to an operational amplifier or other amplifier circuit 90 for amplification prior to being processed in a conventional way by the remainder of the circuitry of the system.

The block diagram of FIG. 6 is illustrated in more detail in FIG. 7 with a detailed schematic diagram. In accordance with a presently preferred embodiment operated at 125 KHz, antenna 70 comprises an 825 uH inductor which is coupled to circuit node 72. Filter 1 (78) from FIG. 6 comprises 1000pF capacitor 92 disposed between node 72 and ground, and 1000 pF capacitor 94 disposed between node 72 and node 84.

In the FSK receive path 76, discriminator 80 comprises diode 94 which is preferably of the type 1N914 but may be any appropriate transistor or diode or other device capable of detecting the AM envelope of the FSK signal. Filter 2 (82) comprises 1000pF capacitor 98 disposed between the cathode of diode 96 and ground along with resistor 100 which is preferably a 100 kilohm resistor disposed between the cathode of diode 96 and ground and resistor 102 which is preferably a 1000 ohm resistor disposed between the cathode of diode 96 and node 84, filter 3 (86) comprises resistor 104 which is preferably a 10 kilohm resistor disposed between node 84 and ground, capacitor 106 which is preferably a .01 uF capacitor disposed between node 84 and ground, a resistor 108 which is preferably a 120 ohm resistor disposed between node 84 and node 110, inductor 112 which is preferably a 1 mH inductor disposed between node 110 and node 88 in parallel with, capacitor 112 and capacitor 114 which are preferably, respectively, 1500 pF and 120 pF capacitors, and finally, capacitor 116 which is preferably a .01 uF capacitor disposed between node 88 and ground.

In accordance with a presently preferred embodiment of the present invention shown in FIG. 10, a switch 117, 118 (such as a transistor, relay or like device) may be incorporated into either or both of PSK branch 74 and FSK branch 76. The switch 117, 118 may be operated by a microprocessor, memory cell 119, or other convenient means well known to those of ordinary skill in the art. The switch may be utilized to enable/disable one or both branches. In this way, for marketing purposes or for other purposes such as security purposes, one branch may be left disabled and the customer could be charged an additional fee for use of an enabler 121 to unlock the remaining signal path, or switch to the other signal path. An enabler 121 could take many forms. Presently preferred is an EEPROM based device which would temporarily mate with a connector on transponder reader 12 to enable FSK operation (for example) and simultaneously decrement a counter in a memory 123 on board the enabler. Once the enabler's counter reached zero, it could not be used again without being reset by the vendor. In this way a premium could be charged for dual mode use and the premium charge could be associated with the sale of or use of the enabler.

Turning now to FIG. 8 depicted there is shown a diagram illustrating the organization of the identification signal stored on transponder 18 as a binary value and transmitted in response to receipt of an interrogation signal by the transponder reader 12. As can be seen, the identification signal is broken into 16 eight bit groups or bytes for a total of 128 bits. Those of ordinary skill in the art will realize that other configurations could be used and that this description applies only to a presently preferred embodiment of the present invention. In accordance with the presently preferred embodiment of the present invention, the bytes are denoted from left to right as follows: S1, S0, D12, D11, D10, D9, D8, D7, D6, D5, D4, D3,

D2, D1, D0, and ED. Bytes S1 and S0 represent the synchronization portion of the identification signal. These are set to the binary value 0000 0000 and 0000 0001 which corresponds to a 0 having even parity and a 0 having odd parity. The data fields D12 through D0 are each configured as seven bits of data followed by a parity bit. Those of ordinary skill in the art will realize that the parity bit could be any of the eight bits. Byte ED is an error detection byte in which is stored an eight bit CRC value calculated over bytes D0 through D12. Such CRC or cyclic redundancy check system are well known to those of ordinary skill in the art. In a presently preferred embodiment of the present invention a 64 bit authorization code number is stored in the identification signal as follows: bit 63 is stored as the first data bit (seventh bit from left) of block D9, bits 62-56 are stored as bits 1-7 of block D8, bits 55-49 are stored as bits 1-7 of block D7, bits 48-42 are stored as bits 1-7 of block D6, bits 41-35 are stored as bits 1-7 of block D5, bits 34-28 are stored as bits 1-7 of block D4, bits 27-21 are stored as bits 1-7 of block D3, bits 20-14 are stored as bits 1-7 of block D2, bits 13-7 are stored as bits 1-7 of block D1 and bits 6-0 are stored as bits 1-7 of block D0. Additional bits in blocks D12, D11, D10 and D9 may be used for various functions including the provision of an output format identification portion of the signal.

In order to provide a variable bit length output from the transponder reader 12 to the controller 14, a single start bit is encoded in the access I.D. portion of the data field (i.e.) D9:1 through D0:1. The start bit immediately follows any necessary leading zeroes and immediately precedes the most significant bit of the authorization code number. It therefore indicates by its position in the field, the number of output bits required.

An example of how the authorization code number is stored in the identification signal follows. Assume that one desires to store authorization code number 8481041 (decimal). This is 816911 in hexadecimal and 1000 0001 0110 1001 0001 0001 in binary. A total of 24 bits are required to store this value. This number must be encoded, however, as a 26-bit number when the two parity bits are appended. Thus the number to encode becomes 01 0000 0010 1101 0010 0010 0011 using the published Security Industry Association 26-Bit Wiegand Reader Interface Standard. Then 26 bits will now occupy bit portions 0 through 25 of the data portion of the identification signal. A Start Bit will be placed at bit position 26 (indicating 26-bit format). The bit pattern (not including data byte parity bits) is thus: 1010 0000 0101 1010 0100 0100 011 with the addition of the Start Bit. Distributing these bits into the 7-data bit/1-parity bit per byte format results in the following:

D5:	0000 0001
D4:	0000 0001

D3:	0101 0001
D2:	0001 0110
D1:	0100 1001
D0:	0100 0110

5           A method of reading the identification signal and simultaneously verifying its validity  
is depicted in FIG. 9. In accordance with the method of FIG. 9, the process starts at block  
120. At block 122 the first number of bits is read. In accordance with the presently preferred  
embodiment of the present invention, this would include a 16 bit group of bits corresponding  
to the length of the synchronization field S0, S1. The bit pattern obtained in block 122 is then  
10          compared with the pre-determined synchronization field to determine if, in fact, it is the  
synchronization field at block 124. The synchronization bit pattern S0, S1 defined above is  
selected because it cannot be duplicated in any of the valid data fields or in the error detection  
field. This is so because of the parity requirement for the data fields D0 through D12. If the  
bit pattern obtained in block 122 is not the synchronization field, control is transferred back to  
15          block 122 where the next bit pattern shifted over one bit from the identification signal is read  
again. If the synchronization field is detected, control transfers to block 126. At block 126  
the next eight bit byte of data is read. At block 128 a parity test is conducted because that byte  
must be one of the data bytes. If the parity test has failed, control transfers back to block 122.  
If the parity test is passed, control transfers to block 130 whereupon the byte is a valid byte  
20          and is stored in a buffer for later use. At block 132, if additional bytes in the data field remain  
to be read, control is transferred back to block 126 in order to read those additional bytes. If  
no additional data bytes remain to be read, then control transfers to block 134 where the error  
detection byte, the final byte in the identification signal, is read. At block 136, the error  
25          detection value is calculated for the bytes that have been stored. This value is then compared at  
block 138 with the error detection value that was read. If the two values are not the same, then  
there is an error and control transfers back to block 122 for additional processing. If no error  
is detected, then control passes to block 140 whereupon the output format determined from the  
identification signal output format identification portion is set in the transponder reader 12 for  
establishing an appropriate protocol for communication with the controller 14. Data is then  
30          transmitted from the transponder reader 12 to the controller 14 in block 142 and the process  
starts anew with control transfer back to block 122.

According to the presently preferred embodiment of the present invention, the error  
35          detection system utilizes a conventional CRC polynomial type error detection system. These  
systems are well known to those of ordinary skill in the art and need not be further described  
herein.

While illustrative embodiments and applications of this invention have been shown and described, it would be apparent to those skilled in the art that many more modifications than have been mentioned above are possible without departing from the inventive concepts set forth herein. The invention, therefore, is not to be limited except in the spirit of the appended  
5 claims.

## CLAIMS

What is claimed is:

1. An electronic transponder for use in a radio frequency identification system, said system including a transponder reader which transmits an interrogation signal and detects a transponder signal having modulated thereon an identification signal transmitted by the transponder in response to detection of the interrogation signal, said transponder comprising:

5 a receiver for receiving said interrogation signal;  
a power circuit for powering the transponder with said received interrogation signal;

and

10 a transmitter, powered by said power circuit responsive to receipt of said interrogation signal, for continuously transmitting an identification signal having a fixed number of binary bits, said identification signal including a synchronization portion having a first number of bits, a data portion having a second number of bits, an output format identification portion having a third number of bits and an error detection portion having a fourth number of bits,

15 said transmitter including means for producing a transponder signal; and  
means for modulating said transponder signal with said identification signal and for transmitting the modulated transponder signal.

20 2. An electronic transponder according to claim 1 wherein said data portion includes a plurality of zeroes followed by a start bit set to one followed by a transponder identification number.

3. An electronic transponder according to claim 1 wherein said data portion includes a plurality of eight-bit bytes, each byte including seven bits of data and one parity bit.

4. An electronic transponder according to claim 3 wherein said parity bit is the least significant bit of each byte.

25 5. An electronic transponder according to claim 1 wherein said data portion and said output format identification portion include a plurality of eight-bit bytes, each byte including data bits and at least one parity bit.

6. An electronic transponder according to claim 5 wherein each said byte includes exactly seven data bits and one parity bit.

7. An electronic transponder according to claim 6 wherein said parity bit is the least significant bit of each byte.

8. An electronic transponder according to claim 7 wherein said parity bit is set to achieve odd parity.

5 9. An electronic transponder according to claim 7 wherein said parity bit is set to achieve even parity.

10. An electronic transponder according to claim 1 wherein said interrogation signal is an RF signal having a first RF frequency.

10 11. An electronic transponder according to claim 10 wherein said first RF frequency is approximately 125 KHz.

12. An electronic transponder according to claim 10 wherein said first RF frequency is approximately 13.56 MHz.

15 13. An electronic transponder according to claim 10 wherein said transponder carrier signal is an RF signal having a second RF frequency, said second RF frequency being lower than said first RF frequency.

14. An electronic transponder according to claim 13 wherein said second RF frequency is a frequency which is an integer fraction of said first RF frequency.

15. An electronic transponder according to claim 14 wherein said first RF frequency is approximately 125 KHz.

20 16. An electronic transponder according to claim 14 wherein said first RF frequency is approximately 13.56 MHz.

17. An electronic transponder according to claim 15 wherein said second RF frequency is approximately 62.5 KHz.

25 18. An electronic transponder according to claim 16 wherein said second RF frequency is approximately one of the frequencies selected from the group consisting of: 6.78

MHz, 4.52 MHz, 3.39 MHz, 2.71 MHz, 2.26 MHz, 1.94 MHz, 1.70 MHz, 1.51 MHz, 1.36 MHz, 1.23 MHz and 1.13 MHz.

5        19. An electronic transponder according to claim 1 wherein said output format identification portion includes at least one bit and specifies a data format that the transponder reader will use to output an authorization code number encoded into said data portion of said identification signal.

20        20. An electronic transponder according to claim 19 wherein said output format identification portion includes four bits.

10        21. An electronic transponder according to claim 1 wherein said identification signal comprises a plurality of eight bit fields, each said eight bit field with the exception of the first, second and last field having a parity bit.

22. An electronic transponder according to claim 21 wherein said synchronization portion comprises the bit pattern: "0000 0000 0000 0001."

15        23. An electronic transponder according to claim 22 wherein said error detection portion is the last field and has eight bits.

24. An electronic transponder according to claim 23 wherein said error detection portion is a cyclic redundancy check value determined by the preceding bits of the data portion and the format identification portion of said identification signal.

25        25. An electronic transponder according to claim 1 wherein said data portion is encrypted.

26. A transponder reader for use in a radio frequency identification system, said system including a transponder which, in response to an interrogation signal, transmits an identification signal, said transponder reader comprising:

means for producing an interrogation signal having a first RF frequency;  
25        circuitry for receiving both PSK and FSK modulated transponder carrier signals on which are modulated the identification signal, the PSK signals having a second RF frequency less than said first RF frequency, and the FSK signals having third and fourth RF frequencies both less than said second RF frequency.

27. A transponder reader for use in a radio frequency identification system, said system including a transponder which, in response to an interrogation signal, transmits an identification signal, said identification signal including an output format identification portion specifying an output format to be used by the transponder reader in communicating with a controller to which it is connected, said transponder reader comprising:

means for producing an interrogation signal having a first RF frequency;

means for receiving a transponder carrier signal transmitted by the transponder and having modulated thereon the identification signal;

means for decoding the identification signal;

means for recognizing the output format identification portion;

means, responsive to the output format identification portion, for selecting an output format to use in communicating with the controller.

28. A transponder reader for use in a radio frequency identification system, said system including a transponder which, in response to an interrogation signal, transmits an identification signal, said transponder reader comprising:

means for producing an interrogation signal having a first RF frequency;

means for receiving a transponder carrier signal having modulated thereon the identification signal, said transponder signal produced by the transponder in response to receipt of the interrogation signal;

said means for receiving including an antenna, a PSK receive path disposed between said antenna and a first circuit node, an FSK receive path disposed between said antenna and said first circuit node, and a first filter for attenuating said first RF frequency disposed between said first circuit node and a second circuit node;

said PSK receive path including a second filter for attenuating said first RF frequency and passing frequencies approximately one-half of said first RF frequency;

said FSK receive path including a discriminator and a third filter, said third filter for attenuating frequencies approximately one-half of said first RF frequency and above and passing RF frequencies less than one-fourth of said first RF frequency.

29. A transponder reader according to claim 28 wherein said first RF frequency is 125 KHz.

30. A transponder reader according to claim 29 wherein said RF frequencies less than one-fourth of said first RF frequency are approximately 15.625 KHz and approximately 12.5 KHz.

31. A method for reading an identification signal from an electronic transponder of a radio frequency identification system, said transponder having stored thereon an identification signal including a synchronization portion having a first number of bits, a data portion having a second number of bits, an output format identification portion having a third number of bits and an error detection portion having a fourth number of bits, said method comprising the steps of:

- (1) reading a first number of bits;
- (2) comparing said first number of bits to a known synchronization bit pattern;
- (3) repeating steps (1) and (2) until a known synchronization bit pattern is detected;
- (4) reading bytes of data from the data portion and the output format identification portion one at a time;
- (5) checking parity in each byte read in step (4);
- (6) returning to step (1) if incorrect parity is detected in step (5);
- (7) storing bytes having correct parity;
- (8) repeating steps (4), (5), (6) and (7) until all bytes in said data portion and said output format identification portion have been read;
- (9) reading the error detection byte;
- (10) calculating an error detection value based upon the bytes stored in step (7);
- (11) comparing the error detection byte read in step (9) with the error detection value calculated in step (10) and determining if they are the same;
- (12) returning to step (1) if they are not the same;
- (13) establishing a communications protocol in communicating with a controller, said communications protocol determined by the output format identification portion; and
- (14) transmitting at least a portion of the data portion to the controller.

32. A method according to claim 31 wherein said error detection byte is a cyclic redundancy check value calculated based upon all bits of the data portion and the output format identification portion of the identification signal.

33. A method according to claim 32 wherein said error detection value is a cyclic redundancy check value calculated based upon all bits of the data portion and the output format identification portion of the read bytes.

34. An electronic transponder for use in a radio frequency identification system, said transponder having stored therein an identification signal, comprising:

a first number of bits of memory for storing a synchronization portion of the identification signal;

5 a second number of bits of memory for storing a data portion of the identification signal;

a third number of bits of memory for storing an output format identification portion of the identification signal; and

10 a fourth number of bits of memory for storing an error detection portion of the identification signal.

35. A transponder according to claim 34 wherein said first number is 16 and said bits are set to 0000 0000 0000 0001.

36. A transponder according to claim 35 wherein said data portion and said format identification portion include 13 8-bit bytes each having 7 bits of data and one parity bit.

15 37. A transponder according to claim 36 wherein said parity bits are the least significant bits of each 8-bit byte.

38. A transponder according to claim 36 wherein said parity bits are the most significant bits of each 8-bit byte.

20 39. A transponder according to claim 37 wherein said error detection portion is a 16th 8-bit byte having no parity bits and comprising a CRC error detection value calculated using the 13 8-bit bytes of said data portion and said format identification portion.

40. A transponder according to claim 38 wherein said error detection portion is a 16th 8-bit byte having no parity bits and comprising a CRC error detection value calculated using the 13 8-bit bytes of said data portion and said format identification portion.

25 41. An RF identification system, comprising:

a transponder reader, including,

interrogating means for generating an RF interrogation signal having a first frequency;

receiving means for receiving and demodulating an identification signal

modulated on an RF transponder signal having a second frequency, said second frequency being lower than said first frequency;

a transponder, including,

5 a memory for storing an identification signal, said identification signal having

a synchronization portion, a data portion having stored therein an authorization code number, an output format identification portion having stored therein an output format identifier specifying an output format to be used by said transponder reader, and an error detection portion;

10 a power circuit for powering said transponder in the presence of said RF interrogation signal;

a frequency divider for generating said RF transponder signal;

15 a transmitter for modulating said identification signal onto said RF transponder signal;

an antenna coupled to said transmitter for radiating said RF transponder signal;

a controller for controlling a peripheral device, said controller including,

15 data communications means having a given data communications protocol for communicating with said transponder reader,

a memory for storing access control criteria;

20 a CPU for comparing said access control criteria with said authorization code number; and

a driver for driving said peripheral device, said CPU activating said driver in response to a comparison of said access control criteria with said authorization code number,

20 said transponder reader communicating with said controller in accordance with said output format specified in said output format identification portion.

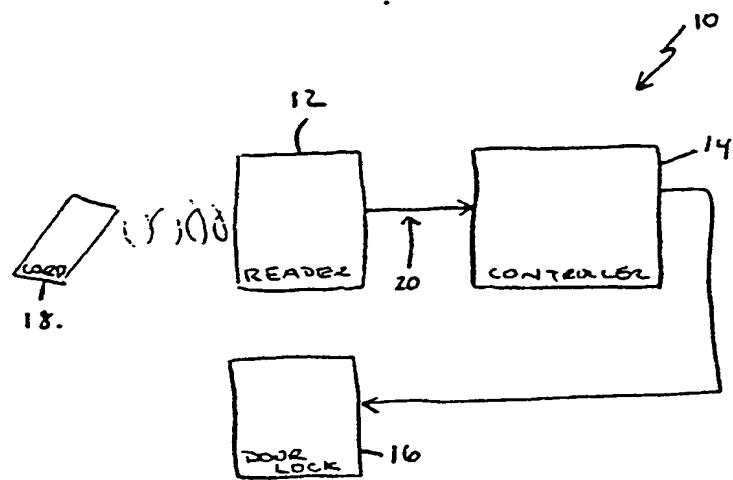


FIG. 1

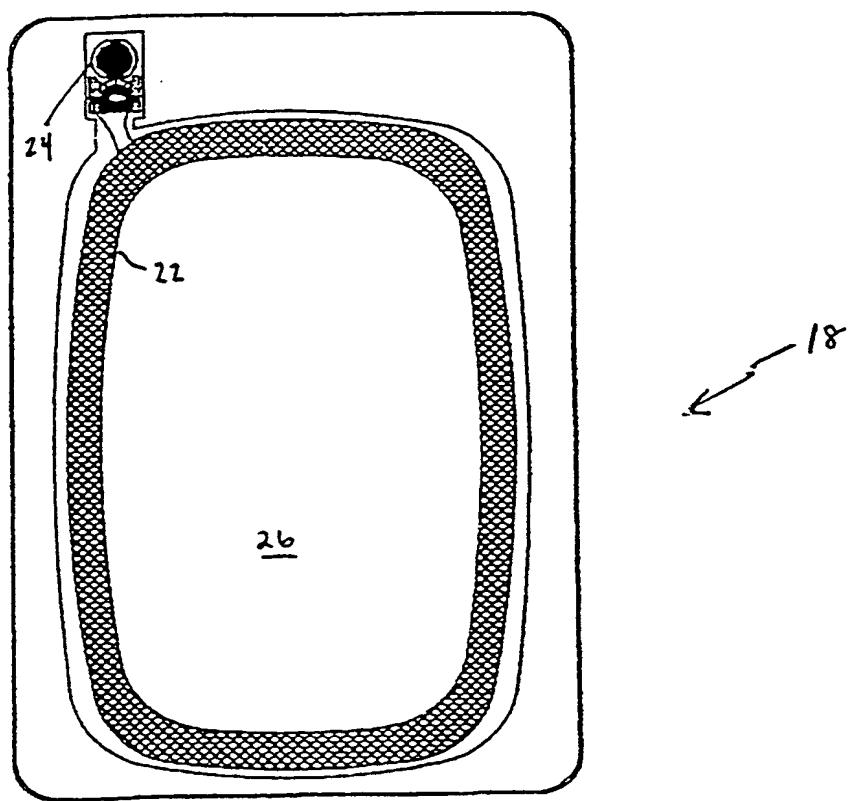


FIG. 2

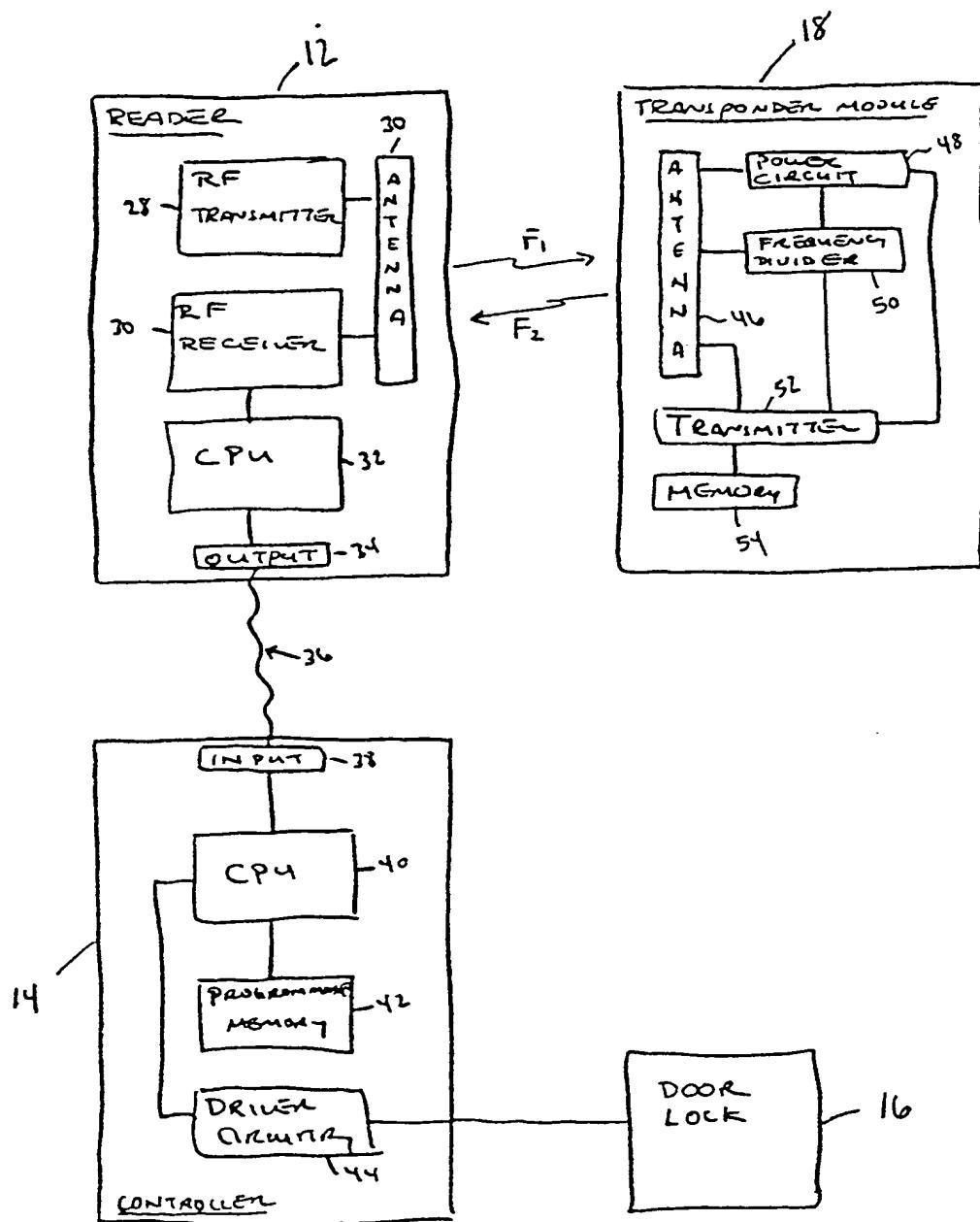


FIG. 3

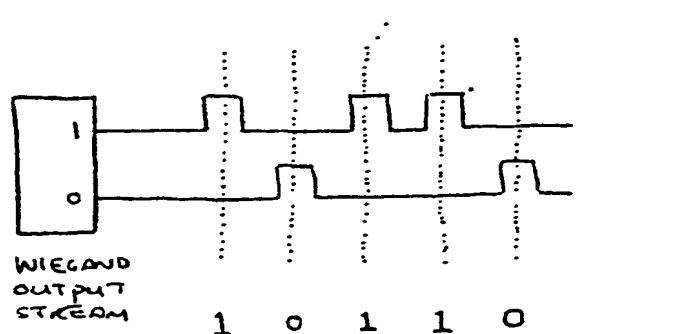


FIG. 4

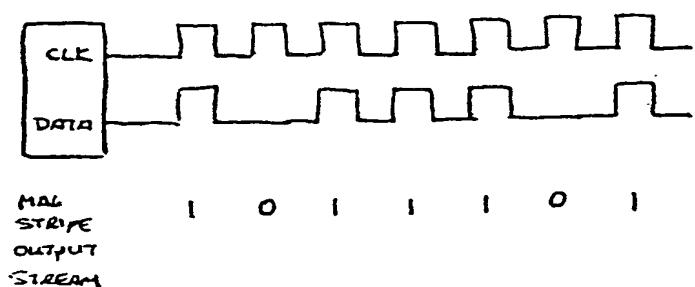
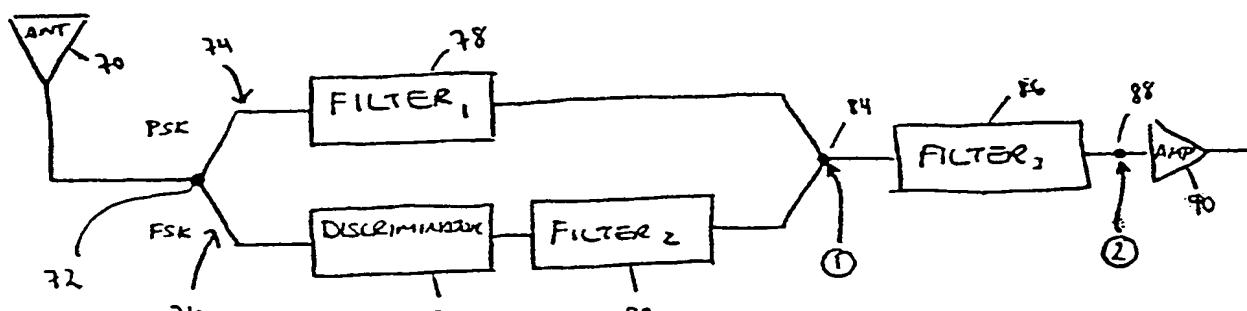


FIG. 5

FIG. 6

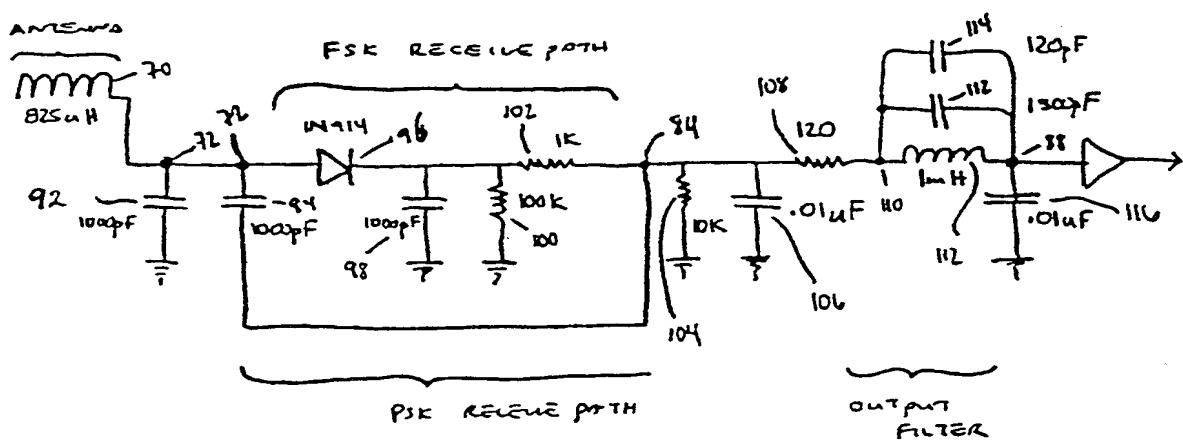
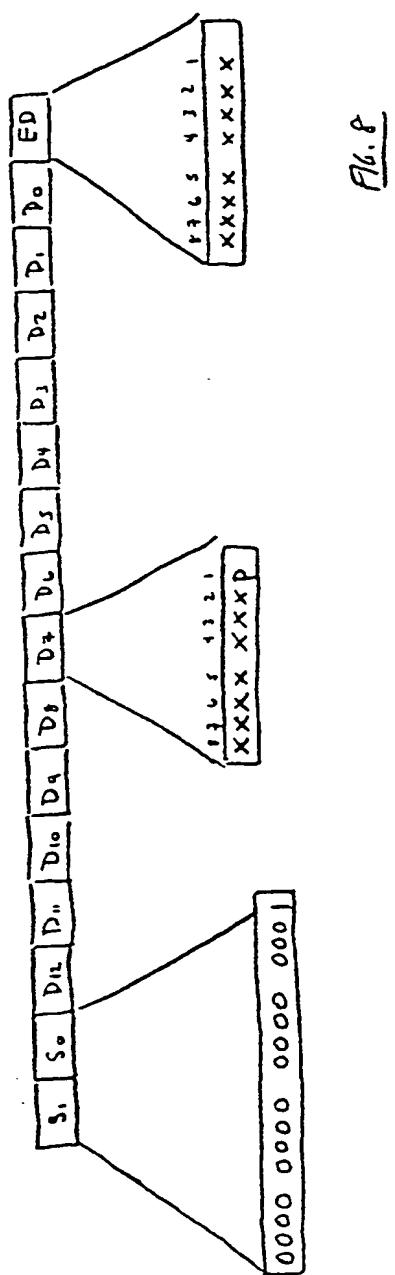
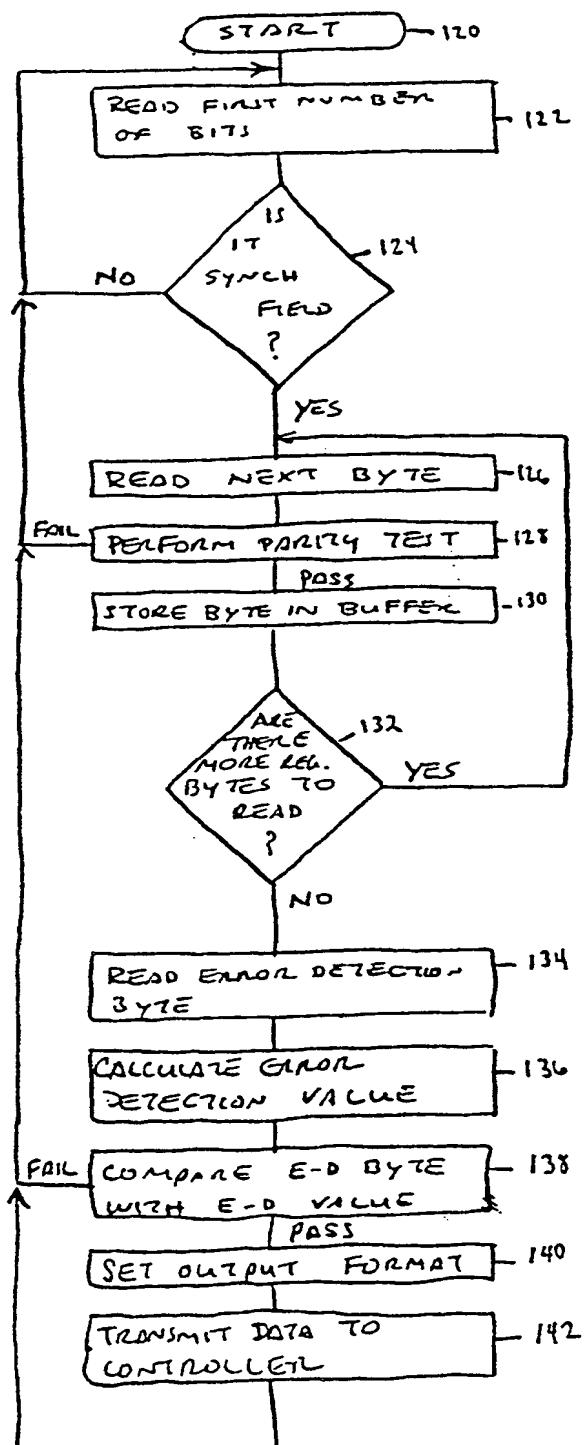


FIG. 7



FIG. 9

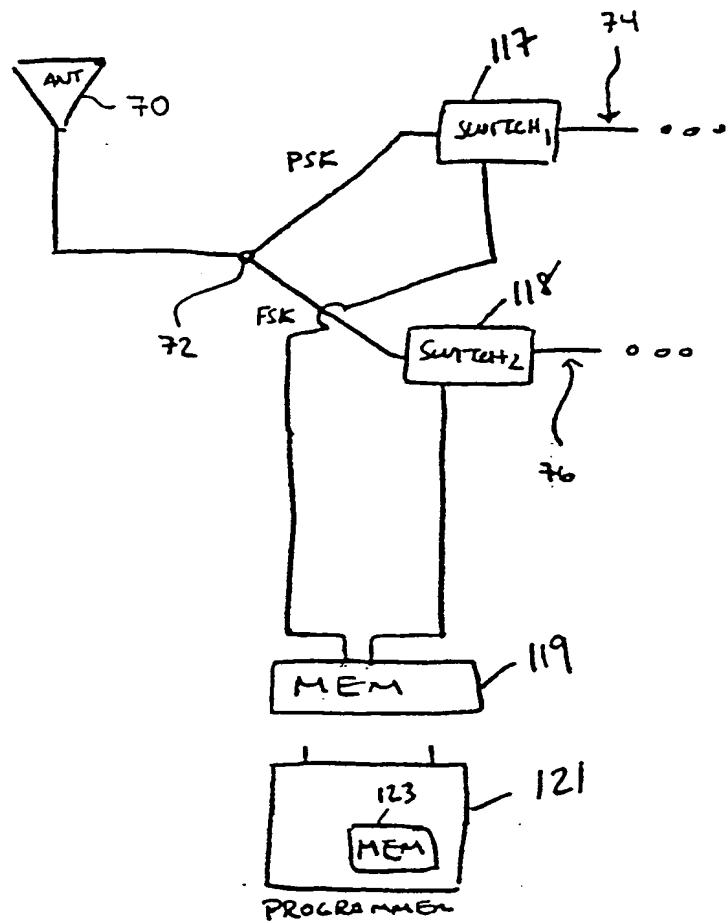


FIG. 10





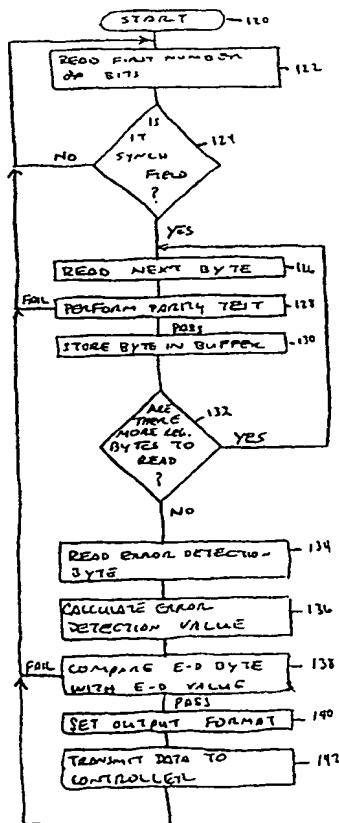
## INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification <sup>7</sup> : <b>G06K 7/00, 17/00</b>		A3	(11) International Publication Number: <b>WO 00/11592</b> (43) International Publication Date: 2 March 2000 (02.03.00)
(21) International Application Number:	PCT/US99/18691	(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).	
(22) International Filing Date:	17 August 1999 (17.08.99)		
(30) Priority Data:	09/138,589 21 August 1998 (21.08.98) US		
(71) Applicant:	KERI SYSTEMS, INCORPORATED [US/US]; Suite 100, 1530 Old Oakland Road, San Jose, CA 95112 (US).		
(72) Inventors:	GEISZLER, Kenneth, J.; 182 Del Prado, Campbell, CA 95008 (US). WALKER, Russel, E.; 4271 North First Street #13, San Jose, CA 95134 (US). WHISTON, Kenneth, Alan; 141 Reed Way, Santa Cruz, CA 95060 (US). KWONG, Jon; 3254 Knight Wood Way, San Jose, CA 95148 (US). LINDSETH, Dale; 138 Pan Tempo Way, Hollister, CA 95023 (US).		
(74) Agents:	D'ALESSANDRO, Kenneth et al.; D'Alessandro & Ritchie, P.O. Box 640640, San Jose, CA 95164-0640 (US).		

## (54) Title: RADIO FREQUENCY IDENTIFICATION SYSTEM

## (57) Abstract

A radio frequency identification system includes a transponder and a transponder reader. The transponder, responsive to an interrogation signal continuously transmitted by the transponder reader, generates a transponder signal modulated by an identification signal readable by the transponder reader. The identification signal includes a synchronization portion, a data portion, an output format identification portion, and an error detection portion. The output format identification portion is used by the reader to configure itself for communication with an attached controller. In another aspect of the invention, the transponder reader may be configured to read FSK as well as PSK encoded signals from the transponder.



**FOR THE PURPOSES OF INFORMATION ONLY**

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece	ML	Mali	TR	Turkey
BG	Bulgaria	HU	Hungary	MN	Mongolia	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MR	Mauritania	UA	Ukraine
BR	Brazil	IL	Israel	MW	Malawi	UG	Uganda
BY	Belarus	IS	Iceland	MX	Mexico	US	United States of America
CA	Canada	IT	Italy	NE	Niger	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NL	Netherlands	VN	Viet Nam
CG	Congo	KE	Kenya	NO	Norway	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NZ	New Zealand	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	PL	Poland		
CM	Cameroon	KR	Republic of Korea	PT	Portugal		
CN	China	KZ	Kazakhstan	RO	Romania		
CU	Cuba	LC	Saint Lucia	RU	Russian Federation		
CZ	Czech Republic	LI	Liechtenstein	SD	Sudan		
DE	Germany	LK	Sri Lanka	SE	Sweden		
DK	Denmark	LR	Liberia	SG	Singapore		
EE	Estonia						

# INTERNATIONAL SEARCH REPORT

Inten. Application No.

PCT/US 99/18691

**A. CLASSIFICATION OF SUBJECT MATTER**  
 IPC 7 G06K7/00 G06K17/00

According to International Patent Classification (IPC) or to both national classification and IPC

**B. FIELDS SEARCHED**

Minimum documentation searched (classification system followed by classification symbols)  
 IPC 7 G01S G07C B61L G06K E05B G07F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the International search (name of data base and, where practical, search terms used)

**C. DOCUMENTS CONSIDERED TO BE RELEVANT**

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5 491 471 A (STOBBE ANATOLI) 13 February 1996 (1996-02-13)	1, 10, 19, 20, 27, 34, 41
Y	column 4, line 46 – line 56 column 5, line 37 – line 44; figures 1-4	5-9, 11-15, 17, 25, 31
Y	column 5, line 57 – line 61	5-9
Y	US 4 650 981 A (FOLETTA WAYNE S) 17 March 1987 (1987-03-17) column 6, line 21 – line 26	11, 13-15, 17 26, 28-30
Y	US 5 521 602 A (BOND MICHAEL X ET AL) 28 May 1996 (1996-05-28)	11, 13-15, 17 26, 28-30
A	abstract; figure 1 column 2, line 38 – line 48	—/—

Further documents are listed in the continuation of box C.

Patent family members are listed in annex.

\* Special categories of cited documents :

- "A" document defining the general state of the art which is not considered to be of particular relevance
- "E" earlier document but published on or after the International filing date
- "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- "O" document referring to an oral disclosure, use, exhibition or other means
- "P" document published prior to the International filing date but later than the priority date claimed

"T" later document published after the International filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the International search

Date of mailing of the International search report

27 March 2000

03.04.2000

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patenttaan 2  
NL - 2280 HV Rijswijk  
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl.  
Fax: (+31-70) 340-9018

Authorized officer

Chiarizia, S

## INTERNATIONAL SEARCH REPORT

Inte	xnal Application No
PCT/US 99/18691	

## C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 4 546 241 A (WALTON CHARLES A) 8 October 1985 (1985-10-08) column 2, line 21 - line 30	12
A		16
Y	EP 0 758 777 A (PALOMAR TECHN CORP) 19 February 1997 (1997-02-19) abstract column 2, line 10 - line 21	25
Y	EP 0 569 131 A (MITSUBISHI ELECTRIC CORP) 10 November 1993 (1993-11-10) column 11, line 10 - line 14 column 11, line 26 - line 36	31
X	US 4 963 887 A (HARUYAMA SHINICHI ET AL) 16 October 1990 (1990-10-16)	26
A	column 5, line 51 -column 6, line 24; figure 2	28-30
P, X	WO 98 52168 A (TROESCH PETER ;CRUZ MICHAEL F (US); LU GUIYANG (US); AVID IDENTIFI) 19 November 1998 (1998-11-19) page 5, line 5 - line 13	26

## **INTERNATIONAL SEARCH REPORT**

International application No.  
**PCT/US 99/18691**

**Box I Observations where certain claims were found unsearchable (Continuation of Item 1 of first sheet)**

This International Search Report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1.  **Claims Nos.:**  
because they relate to subject matter not required to be searched by this Authority, namely:
  
2.  **Claims Nos.:**  
because they relate to parts of the International Application that do not comply with the prescribed requirements to such an extent that no meaningful International Search can be carried out, specifically:
  
3.  **Claims Nos.:**  
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a)

**Box II Observations where unity of invention is lacking (Continuation of Item 2 of first sheet)**

This International Searching Authority found multiple inventions in this international application, as follows:

see additional sheet

- As all required additional search fees were timely paid by the applicant, this International Search Report covers all searchable claims.
- As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.
- As only some of the required additional search fees were timely paid by the applicant, this International Search Report covers only those claims for which fees were paid, specifically claims Nos.:
- No required additional search fees were timely paid by the applicant. Consequently, this International Search Report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

### **Remark on Protect**

The additional search fees were accompanied by the applicant's protest.

No protest accompanied the payment of additional search fees.

FURTHER INFORMATION CONTINUED FROM PCT/ISA/ 210

This International Searching Authority found multiple (groups of) inventions in this international application, as follows:

1. Claims: 1-25, 27 , 31-41

Electronic transponder for use in RF identification system comprising a transmitter for transmitting, and an identifying signal comprising an output format ID portion and parity check portion

2. Claims: 26, 28-30

Transponder reader comprising means for receiving both PSK and FSK modulated signals

A. The special technical features defined in claims 1-25, 27, 31-41 with respect to the document us5491471 are: the features of claim 31 which are not disclosed by said prior art. Namely, the steps of checking parity, solving the objective problem of detecting error in transmission.

B. The special technical features defined in claims 26 and 28 with respect to said prior art. Namely, the means in the reader to deal with PSK as well as FSK, solving the problem of having a reader which is able to deal with transponder of different modulation types.

Thus, there is no common special technical feature to the subjects A and B and these features are neither corresponding features as defined in Rule 13.2 PCT, as they relate to different objectively determined problems and their solutions.

Therefore, the claims do not fulfill the requirements of unity (Rule 13.1 PCT).

**INTERNATIONAL SEARCH REPORT**

Information on patent family members

Inte.	Application No
PCT/US	99/18691

Patent document cited in search report	Publication date	Patent family member(s)		Publication date
US 5491471 A	13-02-1996	DE AT CA DE EP	4134922 C 141430 T 2080716 A 59206907 D 0539763 A	03-12-1992 15-08-1996 24-04-1993 19-09-1996 05-05-1993
US 4650981 A	17-03-1987		NONE	
US 5521602 A	28-05-1996		NONE	
US 4546241 A	08-10-1985		NONE	
EP 0758777 A	19-02-1997	US CA	5832090 A 2182464 A	03-11-1998 11-02-1997
EP 0569131 A	10-11-1993	JP JP DE DE US	2842750 B 5342435 A 69314533 D 69314533 T 5365047 A	06-01-1999 24-12-1993 20-11-1997 19-03-1998 15-11-1993
US 4963887 A	16-10-1990	JP JP CA DE FR GB	2064491 A 2612190 B 1336724 A 3928561 A 2636187 A 2224182 A,B	05-03-1990 21-05-1997 15-08-1995 08-03-1990 09-03-1990 25-04-1990
WO 9852168 A	19-11-1998	AU	7577698 A	08-12-1998

THIS PAGE LEFT BLANK



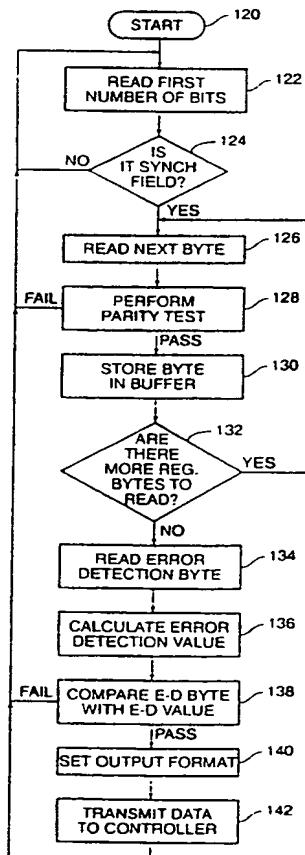
## INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification <sup>7</sup> :	A3	(11) International Publication Number: <b>WO 00/11592</b>
<b>G06K 7/00, 17/00</b>		(43) International Publication Date: 2 March 2000 (02.03.00)
(21) International Application Number: PCT/US99/18691		(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).
(22) International Filing Date: 17 August 1999 (17.08.99)		
(30) Priority Data: 09/138,589 21 August 1998 (21.08.98) US		
(71) Applicant: KERI SYSTEMS, INCORPORATED [US/US]; Suite 100, 1530 Old Oakland Road, San Jose, CA 95112 (US).		
(72) Inventors: GEISZLER, Kenneth, J.; 182 Del Prado, Campbell, CA 95008 (US). WALKER, Russel, E.; 4271 North First Street #13, San Jose, CA 95134 (US). WHISTON, Kenneth, Alan; 141 Reed Way, Santa Cruz, CA 95060 (US). KWONG, Jon; 3254 Knight Wood Way, San Jose, CA 95148 (US). LINDSETH, Dale; 138 Pan Tempo Way, Hollister, CA 95023 (US).		
(74) Agents: D'ALESSANDRO, Kenneth et al.; D'Alessandro & Ritchie, P.O. Box 640640, San Jose, CA 95164-0640 (US).		

## (54) Title: RADIO FREQUENCY IDENTIFICATION SYSTEM

## (57) Abstract

A radio frequency identification system includes a transponder and a transponder reader. The transponder, responsive to an interrogation signal continuously transmitted by the transponder reader, generates a transponder signal modulated by an identification signal readable by the transponder reader. The identification signal includes a synchronization portion, a data portion, an output format identification portion, and an error detection portion. The output format identification portion is used by the reader to configure itself for communication with an attached controller. In another aspect of the invention, the transponder reader may be configured to read FSK as well as PSK encoded signals from the transponder.



**FOR THE PURPOSES OF INFORMATION ONLY**

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece	ML	Mali	TR	Turkey
BG	Bulgaria	HU	Hungary	MN	Mongolia	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MR	Mauritania	UA	Ukraine
BR	Brazil	IL	Israel	MW	Malawi	UG	Uganda
BY	Belarus	IS	Iceland	MX	Mexico	US	United States of America
CA	Canada	IT	Italy	NE	Niger	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NL	Netherlands	VN	Viet Nam
CG	Congo	KE	Kenya	NO	Norway	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NZ	New Zealand	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	PL	Poland		
CM	Cameroon	KR	Republic of Korea	PT	Portugal		
CN	China	KZ	Kazakhstan	RO	Romania		
CU	Cuba	LC	Saint Lucia	RU	Russian Federation		
CZ	Czech Republic	LI	Liechtenstein	SD	Sudan		
DE	Germany	LK	Sri Lanka	SE	Sweden		
DK	Denmark	LR	Liberia	SG	Singapore		
EE	Estonia						

## SPECIFICATION

### TITLE OF THE INVENTION

#### RADIO FREQUENCY IDENTIFICATION SYSTEM

5

### BACKGROUND OF THE INVENTION

#### 1. Field of the Invention

This invention is directed generally to the field of radio frequency RF identification systems employing an electronic transponder and a transponder reader which emits an RF interrogation signal at a first frequency which powers the electronic transponder and enables it to transmit a response on a second frequency (usually a lower frequency). Such systems are used in a number of fields including access security, object identification, inventory control, and generally any field where a small transponder unit may be associated with an object and remotely probed and read by a radio frequency transmission emitted by a transponder reader.

#### 2. The Background Art

Radio frequency identification systems are well known in the art. Such systems are commonly in use in building access schemes where an authorized user of the building is given a building access card containing an authorization code number stored and optionally encrypted on the card as a binary string of data. The card is then presented to a transponder reader which continuously transmits an RF interrogation signal. The card containing a transponder receives the continuously transmitted signal from the transponder reader, uses it to power circuitry on board the card, modulate an RF carrier signal having a different frequency (usually lower) from that of the RF interrogation signal received from the reader (typically an integer fraction of the RF interrogation signal frequency, e.g., 1/2, 1/3, 1/4, etc.) with an identification signal stored on the transponder and containing an authorization code number, and the transponder reader then reads the identification signal emitted from the transponder and passes the authorization code number to an appropriate controller for determining whether or not the authorization code number received is sufficient to allow the user access to the building. If the authorization code number is sufficient, generally a lock will be opened enabling a door to be opened and optionally a computer will log the entry for future reference.

30

Other implementations of such systems enable object identification by reading a

transponder attached to or embedded in the object (e.g., cargo identification, pet identification, taxi identification at an airport, and the like).

Generally, all existing transponder readers of such radio frequency identification systems utilize proprietary systems. That is, a card from one system will not be readable by a system provided by another vendor. In some systems, the transponder emits a signal modulated by frequency shift keying (FSK), i.e., the binary transmission is represented by a mark and a space which correspond to the 1 and 0 of the binary signal, the mark and space being signals on two separate frequencies (e.g., 1/8 and 1/10 of the frequency of the RF interrogation signal). Other systems utilize phase shift keying (PSK) as well known in the art.

Systems using PSK modulation cannot read the cards which transmit FSK modulated information and systems which read FSK modulated information cannot read the cards which transmit PSK modulated information.

While all such transponder readers read matching transponder cards, in most systems they are also required to communicate with a controller of some sort. The controller generally comprises a central processing unit (CPU) which may interact with a number of such readers which are simultaneously connected to it. A number of different systems have evolved over the years for communicating data from a reader to a controller. Some of these systems, or communications protocols, are known as magnetic stripe communications protocol, Wiegand communications protocol, single wire Wiegand communications protocol, RS232 communications protocol, RS422 communications protocol, and the like. These various communication protocols generally require 1, 2, 3 or more electrical wire connections between the transponder reader and the controller. Furthermore, the data modulation schemes for these various systems differ as well known to those of ordinary skill in the art. This has led to a problem in the industry in the stocking of transponder readers. In order to stock transponder readers which are compatible with the various communications protocols employed by the various controllers, one needs to stock many transponder readers which are mutually incompatible with one another. A need, therefore, exists for a transponder reader which is capable of working with a number of different communication protocols in communicating with a corresponding controller so as to reduce the inventory requirements for transponder readers.

It is also desirable to have the transponder reader require as little field programming as possible. In this way, relatively unskilled personnel may successfully install transponder readers and have them operate with corresponding controllers and transponders with relatively little difficulty. To avoid the necessity to physically program such readers to communicate

using a given communications protocol (as by setting DIP switches or jumpers) would be highly desirable.

#### OBJECTS AND ADVANTAGES OF THE INVENTION

Accordingly, it is an object and advantage of the present invention to provide an  
5 improved RF identification system.

It is a further object and advantage of the present invention to provide an improved transponder reader for use in RF identification systems.

It is a further object and advantage of the present invention to provide a capability to  
10 program the transponder reader to communicate with an attached controller using a communications protocol specified by information contained in an output format identification portion of the identification signal stored in the transponder and transmitted to the transponder reader.

It is a further object and advantage of the present invention to provide an improved  
15 transponder for use in an RF identification system.

It is a further object and advantage of the present invention to provide a transponder for  
use in an RF identification system which contains an identification signal which has within it,  
in addition to an authorization code number, an output format identification portion which,  
when transmitted to and received by the transponder reader, defines the communications  
20 protocol to be used by the  
transponder reader in communicating with attached devices such as a controller.

Yet another object and advantage of the present invention is the provision of a  
transponder reader capable of reading both PSK and FSK signals.

Yet another object and advantage of the present invention is the provision of a  
25 mechanism by which either the PSK or the FSK mode of operation may be normally disabled  
and easily authorized in an accountable manner.

These and many other objects and advantages of the present invention will become  
apparent to those of ordinary skill in the art from a consideration of the drawings and ensuing  
description of the invention.

## SUMMARY OF THE INVENTION

A radio frequency identification system includes a transponder and a transponder reader. The transponder, responsive to an interrogation signal continuously transmitted by the transponder reader, generates a transponder signal modulated by an identification signal readable by the transponder reader. The identification signal includes a synchronization portion, a data portion, an output format identification portion, and an error detection portion. The output format identification portion is used by the reader to configure itself for communication with an attached controller. In another aspect of the invention, the transponder reader may be configured to read FSK as well as PSK encoded signals from the transponder.

## BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a system block diagram of an RF identification system in accordance with a presently preferred embodiment of the present invention.

FIG. 2 is a sectional top plan view of a transponder card in accordance with a presently preferred embodiment of the present invention.

FIG. 3 is a detailed system block diagram of an RF identification system in accordance with a presently preferred embodiment of the present invention.

FIG. 4 is a timing and data output diagram for a conventional Wiegand output data stream.

FIG. 5 is a timing and data output diagram for a conventional mag stripe output data stream.

FIG. 6 is a block diagram of a circuit for receiving transponder signals modulated with either PSK or FSK modulation techniques in accordance with a presently preferred embodiment of the present invention.

FIG. 7 is a detailed circuit diagram for circuit for receiving transponder signals modulated with either PSK or FSK modulation techniques in accordance with a presently

preferred embodiment of the present invention.

FIG. 8 is a diagram showing the layout of data stored on a transponder card in accordance with a presently preferred embodiment of the present invention.

5 FIG. 9 is a flow chart diagraming a method for reading and verifying data received from a transponder card in accordance with a presently preferred embodiment of the present invention.

10 FIG. 10 is a partial block diagram of a modification of the circuit of FIG. 6 in which programmable switches control the flow of RF signal through the PSK and FSK signal processing branches of the transponder reader in accordance with a presently preferred embodiment of the present invention.

#### DESCRIPTION OF THE PREFERRED EMBODIMENTS

Those of ordinary skill in the art will realize that the following description of the present invention is illustrative only and is not intended to be in any way limiting. Other 15 embodiments of the invention will readily suggest themselves to such skilled persons from an examination of the within disclosure.

The present invention is directed to a radio frequency (RF) identification system which solves many problems of the prior art. Turning now to Fig. 1, a system diagram of a radio frequency identification system generally denoted 10 in accordance with a presently preferred embodiment of the present invention is shown. System 10 includes a transponder reader 12, a controller 14, and something controlled by the controller such as a door lock 16, and a transponder 18. As with all such radio frequency identification systems, transponder reader 12 preferably continuously emits a radio frequency interrogation signal of a given frequency. According to presently preferred embodiments of the present invention, the interrogation 20 signal is either at approximately 125 KHz or at approximately 13.56 MHz although those of ordinary skill in the art will realize that virtually any other frequency in the RF spectrum could be used. The radio frequency signal is received by transponder 18 which includes an antenna and a rectifier circuit or "power circuit" for deriving electrical power from the received signal. Transponder 18 then transmits, in response to receipt of the interrogation signal from 25 transponder reader 12, a transponder signal of a lower frequency than the interrogation signal having modulated thereon a stored identification signal in the form of a binary data stream. As long as the transponder 18 is close enough to transponder reader 12 that it can receive the 30

interrogation signal therefrom, it will also continuously transmit a transponder signal which can then be picked up by the transponder reader 12 and demodulated.

Upon demodulating the transponder signal, transponder reader 12 obtains therefrom the identification signal originally stored on card 18. A portion of the identification signal is an authorization code number. That authorization code number is passed from transponder reader 12 to controller 14 over data communication line 20 in accordance with a given data communications protocol. In accordance with a presently preferred embodiment of the present invention, the data communications protocol used over line 20 is specified by an output format identification portion of the identification signal transmitted from transponder 18 to transponder reader 12. The protocol may be preferably one of several well known in the art such as, for example, RS232, RS422, various versions of the Wiegand protocol, and various versions of the mag stripe protocol. Other protocols may also be specified and used where appropriate.

The ability to store the selected data communications protocol to be used by a transponder reader 12 reading the transponder at the time of initially programming the transponder 18 permits a single transponder reader 12 to be used with a variety of controllers 14 and avoids the necessity for stocking a number of different transponder readers each compatible with a particular controller system.

Upon receipt of a valid authorization code number over line 20, controller 14 then activates door lock 16 or other appropriate apparatus as well known to those of ordinary skill in the art.

Turning now to FIG. 2, a top view of a typical transponder 18 is shown. Transponder 18 comprises an antenna 22 connected to a transponder integrated circuit 24 all preferably embedded within a plastic card or tag 26 or otherwise encapsulated. According to a presently preferred embodiment of the present invention, the integrated circuit is a Micro Chip Technology MCRCF250 or MCRCF350. The MCRCF250 operates at 125 KHz and the MCRCF350 operates at 13.56 MHz. Those of ordinary skill in the art will realize that this particular integrated circuit can be substituted for individual components or other integrated circuits made by other manufacturers in order to achieve the same purpose and function. Micro Chip Technology, Inc. is located in Chandler, Arizona and on the World Wide Web at [www.microchip.com](http://www.microchip.com).

Turning now to FIG. 3, a detailed block diagram of a system in accordance with the present invention is shown. Reader or transponder reader 12 includes an RF transmitter section 28 which generates an RF carrier signal which is coupled to antenna 30 for transmission from reader transponder 12. Also coupled to antenna 30 is an RF receiver section 31 for receiving and demodulating signals received from the transponder 18 over antenna 30. Coupled to the RF receiver section 31 is a CPU 32 which processes and demodulates the identification signal received from the transponder 18 and sets the communications protocol to be used in communicating between transponder reader 12 and controller 14 in accordance with an output format identification portion of the identification signal received from the transponder module 18. CPU 32 is coupled to conventional output drivers 34 and a data link 36 communicating with controller 14.

Controller 14 includes typical input circuitry 38 coupled to a conventional CPU 40 which is in turn coupled to programmable memory 42 for storing access criteria to be compared with the authorization code number received from the transponder reader 12. CPU 40 is also coupled to driver circuitry 44 of a conventional nature for driving a door lock or other associated apparatus 16 upon determination by CPU 40 that access is permitted. Those of ordinary skill in the art will also realize that this system can easily be adapted to systems for inventory control and object identification and tracking, e.g., by recording the presence of a serial number received from a transponder module rather than by opening a door lock.

Transponder 18 comprises an antenna 46 coupled to a power circuit 48 which rectifies a received interrogation signal from transponder reader 12 to power the circuitry of transponder 18. Also coupled to antenna 46 is a frequency divider circuit 50 for providing a carrier signal to transmitter 52 (also coupled to antenna 46). Frequency divider 50 provides a signal used by transmitter 52 to modulate an identification signal onto. The identification signal is preferably stored as a binary 128 bit value in memory 54. Those of ordinary skill in the art will realize that other numbers of bits could be used as could non-binary values. Memory 54 is preferably a one time programmable memory cell, such as an EEPROM. Upon activation by the presence of an interrogation signal, transmitter 52 transmits an identification signal modulated onto a carrier at an integer fraction of the interrogation signal. For a 125 KHz system (i.e., one operating with an interrogation signal of 125 KHz), the transponder signal in PSK mode is at approximately 62.5 KHz and in FSK mode is at 12.5 KHz and 15.625 KHz for the mark and space (the one that is the mark and the one that is the space are a matter of choice for the developer).

Turning now to FIG. 4, the output of a Wiegand output stream is depicted. In the

Wiegand output protocol there are two active lines, one associated with the binary value 1 and the other associated with the binary value 0. To indicate the presence of a 1, the 1 line goes high and the 0 line stays low. To indicate the value of 0, the 0 line goes high and the 1 line stays low. FIG. 4 indicates the manner in which the binary value 10110 would be transmitted over this pair of lines.

FIG. 5 shows data transmission in accordance with the conventional mag stripe output protocol. In the mag stripe protocol, there are two lines for conveying data, one is a clock line (CLK) and one is a data line (DATA). The clock line generates a pulse at a regular time interval. The data line generates a pulse corresponding with a clock pulse to represent a 1 and the lack of a pulse corresponding with a clock pulse indicates a 0. The signals shown in FIG. 5 indicate how the binary value 1011101 would be transmitted over this pair of lines in a conventional mag stripe output protocol.

Those of ordinary skill in the art will realize that there are a number of different ways to transmit such data including RS422, RS232, various versions of the mag stripe output stream format including open collector versions thereof and various versions of the Wiegand output stream format including open collector versions thereof and single wire versions thereof. The advantage of this aspect of the present invention is that the transponder reader 12 can be simply programmed by the transponder to output data to the controller 14 in any one of a number of different data communications protocols by simply setting the output format identification portion of the identification signal stored on the transponder 18 to the correct value corresponding to that particular communications protocol.

In practice, an installer would purchase a transponder reader 12 in accordance with the present invention and connect it to an existing controller 14 having a given data communications protocol. The transponders 18 would then all be programmed in accordance with the controller's requirements. A data communications protocol would be specified in the output format identification portion of the identification signal stored on the transponder 18 (this value is not passed to the controller 14). Where the card is read, the reader automatically passes only the authorization code number to the controller 14 in accordance with the specified protocol.

Turning now to FIG. 6, an additional aspect of the invention is disclosed. Because most transponders used in RF identification systems use either phase shift keying (PSK) or frequency shift keying (FSK), it has usually been the case that transponders and transponder readers had to comport with one standard or the other standard, i.e., PSK or FSK. No prior

known systems are capable of dual mode operation. In accordance with the present invention, however, the front end of the reader comprises two distinct signal processing paths. The first path processes PSK signals and the second path processes FSK signals. Generally, PSK signals are at a carrier frequency of one-half (or another integer fraction) of the interrogation signal frequency. That means, for an interrogation signal frequency of 125 KHz, the transponder's response PSK signal would be at 62.5 KHz. FSK signals, on the other hand, commonly have a mark signal and a space signal, one of the mark and space signals being at one-eighth the interrogation signal frequency and the other being at one-tenth the interrogation signal frequency. Other frequency shifts may be used. Thus, an FSK signal might have a mark at 12.5 KHz, and a space at 15.625 KHz, or vice versa. It is therefore possible, with filters, to direct the two signal trains through different branches of a circuit for processing.

Turning now to FIG. 6, an antenna 70 associated with the transponder reader 12 receives a signal from transponder 18 and passes it to circuit node 72. At circuit node 72, the signal will pass along branch 74 if it is a PSK signal, i.e., it has a first frequency less than the frequency of the interrogation signal. Similarly, the signal will pass along branch 76 for FSK processing if it has a frequency less than that of a PSK signal. In this example, assuming that the interrogation signal is a 125 KHz signal, 62.5 KHz signals will pass along the PSK branch 74 and 12-15 KHz signals will pass along the FSK branch 76. This is made possible by the use of filters. Filter No. 1 (78) is designed to pass frequencies consistent with the PSK signal pass band. In this example, those frequencies would be near 62.5 KHz. Filter 78 is designed to reject frequencies at 125 KHz as well as to reject frequencies significantly below 62.5 KHz, such as a FSK signals at 12-16 KHz. Turning to the FSK processing branch 76, discriminator 80 is used in a conventional manner to discriminate or AM envelope detect the mark and space FSK signals at 12-16 KHz. Filter No. 2 (82) is designed to stop 125 KHz signals but to pass those signals in the range of 12-16 KHz. The PSK and FSK branches 74 and 76 rejoin at node 1 (84) and are then passed through filter no. 3 (86) which also rejects 125 KHz signals whereupon they reach node 2 (88) and are input to an operational amplifier or other amplifier circuit 90 for amplification prior to being processed in a conventional way by the remainder of the circuitry of the system.

The block diagram of FIG. 6 is illustrated in more detail in FIG. 7 with a detailed schematic diagram. In accordance with a presently preferred embodiment operated at 125 KHz, antenna 70 comprises an 825 uH inductor which is coupled to circuit node 72. Filter 1 (78) from FIG. 6 comprises 1000pF capacitor 92 disposed between node 72 and ground, and 1000 pF capacitor 94 disposed between node 72 and node 84.

In the FSK receive path 76, discriminator 80 comprises diode 94 which is preferably of the type 1N914 but may be any appropriate transistor or diode or other device capable of detecting the AM envelope of the FSK signal. Filter 2 (82) comprises 1000pF capacitor 98 disposed between the cathode of diode 96 and ground along with resistor 100 which is preferably a 100 kilohm resistor disposed between the cathode of diode 96 and ground and resistor 102 which is preferably a 1000 ohm resistor disposed between the cathode of diode 96 and node 84, filter 3 (86) comprises resistor 104 which is preferably a 10 kilohm resistor disposed between node 84 and ground, capacitor 106 which is preferably a .01  $\mu$ F capacitor disposed between node 84 and ground, a resistor 108 which is preferably a 120 ohm resistor disposed between node 84 and node 110, inductor 111 which is preferably a 1 mH inductor disposed between node 110 and node 88 in parallel with, capacitor 112 and capacitor 114 which are preferably, respectively, 1500 pF and 120 pF capacitors, and finally, capacitor 116 which is preferably a .01  $\mu$ F capacitor disposed between node 88 and ground.

In accordance with a presently preferred embodiment of the present invention shown in FIG. 10, a switch 117, 118 (such as a transistor, relay or like device) may be incorporated into either or both of PSK branch 74 and FSK branch 76. The switch 117, 118 may be operated by a microprocessor, memory cell 119, or other convenient means well known to those of ordinary skill in the art. The switch may be utilized to enable/disable one or both branches. In this way, for marketing purposes or for other purposes such as security purposes, one branch may be left disabled and the customer could be charged an additional fee for use of an enabler 121 to unlock the remaining signal path, or switch to the other signal path. An enabler 121 could take many forms. Presently preferred is an EEPROM based device which would temporarily mate with a connector on transponder reader 12 to enable FSK operation (for example) and simultaneously decrement a counter in a memory 123 on board the enabler. Once the enabler's counter reached zero, it could not be used again without being reset by the vendor. In this way a premium could be charged for dual mode use and the premium charge could be associated with the sale of or use of the enabler.

Turning now to FIG. 8 depicted there is shown a diagram illustrating the organization of the identification signal stored on transponder 18 as a binary value and transmitted in response to receipt of an interrogation signal by the transponder reader 12. As can be seen, the identification signal is broken into 16 eight bit groups or bytes for a total of 128 bits. Those of ordinary skill in the art will realize that other configurations could be used and that this description applies only to a presently preferred embodiment of the present invention. In accordance with the presently preferred embodiment of the present invention, the bytes are denoted from left to right as follows: S1, S0, D12, D11, D10, D9, D8, D7, D6, D5, D4, D3,

D2, D1, D0, and ED. Bytes S1 and S0 represent the synchronization portion of the identification signal. These are set to the binary value 0000 0000 and 0000 0001 which corresponds to a 0 having even parity and a 0 having odd parity. The data fields D12 through D0 are each configured as seven bits of data followed by a parity bit. Those of ordinary skill in the art will realize that the parity bit could be any of the eight bits. Byte ED is an error detection byte in which is stored an eight bit CRC value calculated over bytes D0 through D12. Such CRC or cyclic redundancy check system are well known to those of ordinary skill in the art. In a presently preferred embodiment of the present invention a 64 bit authorization code number is stored in the identification signal as follows: bit 63 is stored as the first data bit (seventh bit from left) of block D9, bits 62-56 are stored as bits 1-7 of block D8, bits 55-49 are stored as bits 1-7 of block D7, bits 48-42 are stored as bits 1-7 of block D6, bits 41-35 are stored as bits 1-7 of block D5, bits 34-28 are stored as bits 1-7 of block D4, bits 27-21 are stored as bits 1-7 of block D3, bits 20-14 are stored as bits 1-7 of block D2, bits 13-7 are stored as bits 1-7 of block D1 and bits 6-0 are stored as bits 1-7 of block D0. Additional bits in blocks D12, D11, D10 and D9 may be used for various functions including the provision of an output format identification portion of the signal.

In order to provide a variable bit length output from the transponder reader 12 to the controller 14, a single start bit is encoded in the access I.D. portion of the data field (i.e.) D9:1 through D0:1. The start bit immediately follows any necessary leading zeroes and immediately precedes the most significant bit of the authorization code number. It therefore indicates by its position in the field, the number of output bits required.

An example of how the authorization code number is stored in the identification signal follows. Assume that one desires to store authorization code number 8481041 (decimal). This is 816911 in hexadecimal and 1000 0001 0110 1001 0001 0001 in binary. A total of 24 bits are required to store this value. This number must be encoded, however, as a 26-bit number when the two parity bits are appended. Thus the number to encode becomes 01 0000 0010 1101 0010 0010 0011 using the published Security Industry Association 26-Bit Wiegand Reader Interface Standard. Then 26 bits will now occupy bit portions 0 through 25 of the data portion of the identification signal. A Start Bit will be placed at bit position 26 (indicating 26-bit format). The bit pattern (not including data byte parity bits) is thus: 1010 0000 0101 1010 0100 0100 011 with the addition of the Start Bit. Distributing these bits into the 7-data bit/1-parity bit per byte format results in the following:

D5:	0000 0001
D4:	0000 0001

D3:	0101 0001
D2:	0001 0110
D1:	0100 1001
D0:	0100 0110

5        A method of reading the identification signal and simultaneously verifying its validity is depicted in FIG. 9. In accordance with the method of FIG. 9, the process starts at block 120. At block 122 the first number of bits is read. In accordance with the presently preferred embodiment of the present invention, this would include a 16 bit group of bits corresponding to the length of the synchronization field S0, S1. The bit pattern obtained in block 122 is then  
10      compared with the pre-determined synchronization field to determine if, in fact, it is the synchronization field at block 124. The synchronization bit pattern S0, S1 defined above is selected because it cannot be duplicated in any of the valid data fields or in the error detection field. This is so because of the parity requirement for the data fields D0 through D12. If the bit pattern obtained in block 122 is not the synchronization field, control is transferred back to block 122 where the next bit pattern shifted over one bit from the identification signal is read again. If the synchronization field is detected, control transfers to block 126. At block 126  
15      the next eight bit byte of data is read. At block 128 a parity test is conducted because that byte must be one of the data bytes. If the parity test has failed, control transfers back to block 122. If the parity test is passed, control transfers to block 130 whereupon the byte is a valid byte and is stored in a buffer for later use. At block 132, if additional bytes in the data field remain to be read, control is transferred back to block 126 in order to read those additional bytes. If no additional data bytes remain to be read, then control transfers to block 134 where the error  
20      detection byte, the final byte in the identification signal, is read. At block 136, the error detection value is calculated for the bytes that have been stored. This value is then compared at block 138 with the error detection value that was read. If the two values are not the same, then there is an error and control transfers back to block 122 for additional processing. If no error  
25      is detected, then control passes to block 140 whereupon the output format determined from the identification signal output format identification portion is set in the transponder reader 12 for establishing an appropriate protocol for communication with the controller 14. Data is then  
30      transmitted from the transponder reader 12 to the controller 14 in block 142 and the process starts anew with control transfer back to block 122.

According to the presently preferred embodiment of the present invention, the error detection system utilizes a conventional CRC polynomial type error detection system. These systems are well known to those of ordinary skill in the art and need not be further described  
35      herein.

While illustrative embodiments and applications of this invention have been shown and described, it would be apparent to those skilled in the art that many more modifications than have been mentioned above are possible without departing from the inventive concepts set forth herein. The invention, therefore, is not to be limited except in the spirit of the appended claims.

5

## CLAIMS

What is claimed is:

1. An electronic transponder for use in a radio frequency identification system, said system including a transponder reader which transmits an interrogation signal and detects a transponder signal having modulated thereon an identification signal transmitted by the transponder in response to detection of the interrogation signal, said transponder comprising:
  - a receiver for receiving said interrogation signal;
  - a power circuit for powering the transponder with said received interrogation signal; and

10 a transmitter, powered by said power circuit responsive to receipt of said interrogation signal, for continuously transmitting an identification signal having a fixed number of binary bits, said identification signal including a synchronization portion having a first number of bits, a data portion having a second number of bits, an output format identification portion having a third number of bits and an error detection portion having a fourth number of bits,

15 said transmitter including means for producing a transponder signal; and means for modulating said transponder signal with said identification signal and for transmitting the modulated transponder signal.
2. An electronic transponder according to claim 1 wherein said data portion includes a plurality of zeroes followed by a start bit set to one followed by a transponder identification number.
3. An electronic transponder according to claim 1 wherein said data portion includes a plurality of eight-bit bytes, each byte including seven bits of data and one parity bit.
4. An electronic transponder according to claim 3 wherein said parity bit is the least significant bit of each byte.
- 25 5. An electronic transponder according to claim 1 wherein said data portion and said output format identification portion include a plurality of eight-bit bytes, each byte including data bits and at least one parity bit.
6. An electronic transponder according to claim 5 wherein each said byte includes exactly seven data bits and one parity bit.

7. An electronic transponder according to claim 6 wherein said parity bit is the least significant bit of each byte.

8. An electronic transponder according to claim 7 wherein said parity bit is set to achieve odd parity.

5 9. An electronic transponder according to claim 7 wherein said parity bit is set to achieve even parity.

10. An electronic transponder according to claim 1 wherein said interrogation signal is an RF signal having a first RF frequency.

10 11. An electronic transponder according to claim 10 wherein said first RF frequency is approximately 125 KHz.

12. An electronic transponder according to claim 10 wherein said first RF frequency is approximately 13.56 MHz.

15 13. An electronic transponder according to claim 10 wherein said transponder carrier signal is an RF signal having a second RF frequency, said second RF frequency being lower than said first RF frequency.

14. An electronic transponder according to claim 13 wherein said second RF frequency is a frequency which is an integer fraction of said first RF frequency.

15. An electronic transponder according to claim 14 wherein said first RF frequency is approximately 125 KHz.

20 16. An electronic transponder according to claim 14 wherein said first RF frequency is approximately 13.56 MHz.

17. An electronic transponder according to claim 15 wherein said second RF frequency is approximately 62.5 KHz.

25 18. An electronic transponder according to claim 16 wherein said second RF frequency is approximately one of the frequencies selected from the group consisting of: 6.78

MHz, 4.52 MHz, 3.39 MHz, 2.71 MHz, 2.26 MHz, 1.94 MHz, 1.70 MHz, 1.51 MHz, 1.36 MHz, 1.23 MHz and 1.13 MHz.

19. An electronic transponder according to claim 1 wherein said output format identification portion includes at least one bit and specifies a data format that the transponder reader will use to output an authorization code number encoded into said data portion of said identification signal.

20. An electronic transponder according to claim 19 wherein said output format identification portion includes four bits.

21. An electronic transponder according to claim 1 wherein said identification signal comprises a plurality of eight bit fields, each said eight bit field with the exception of the first, second and last field having a parity bit.

22. An electronic transponder according to claim 21 wherein said synchronization portion comprises the bit pattern: "0000 0000 0000 0001."

23. An electronic transponder according to claim 22 wherein said error detection portion is the last field and has eight bits.

24. An electronic transponder according to claim 23 wherein said error detection portion is a cyclic redundancy check value determined by the preceding bits of the data portion and the format identification portion of said identification signal.

25. An electronic transponder according to claim 1 wherein said data portion is encrypted.

26. A transponder reader for use in a radio frequency identification system, said system including a transponder which, in response to an interrogation signal, transmits an identification signal, said transponder reader comprising:

means for producing an interrogation signal having a first RF frequency;

25 circuitry for receiving both PSK and FSK modulated transponder carrier signals on which are modulated the identification signal, the PSK signals having a second RF frequency less than said first RF frequency, and the FSK signals having third and fourth RF frequencies both less than said second RF frequency.

27. A transponder reader for use in a radio frequency identification system, said system including a transponder which, in response to an interrogation signal, transmits an identification signal, said identification signal including an output format identification portion specifying an output format to be used by the transponder reader in communicating with a controller to which it is connected, said transponder reader comprising:

means for producing an interrogation signal having a first RF frequency;

means for receiving a transponder carrier signal transmitted by the transponder and having modulated thereon the identification signal;

means for decoding the identification signal;

means for recognizing the output format identification portion;

means, responsive to the output format identification portion, for selecting an output format to use in communicating with the controller.

28. A transponder reader for use in a radio frequency identification system, said system including a transponder which, in response to an interrogation signal, transmits an identification signal, said transponder reader comprising:

means for producing an interrogation signal having a first RF frequency;

means for receiving a transponder carrier signal having modulated thereon the identification signal, said transponder signal produced by the transponder in response to receipt of the interrogation signal;

said means for receiving including an antenna, a PSK receive path disposed between said antenna and a first circuit node, an FSK receive path disposed between said antenna and said first circuit node, and a first filter for attenuating said first RF frequency disposed between said first circuit node and a second circuit node;

said PSK receive path including a second filter for attenuating said first RF frequency and passing frequencies approximately one-half of said first RF frequency;

said FSK receive path including a discriminator and a third filter, said third filter for attenuating frequencies approximately one-half of said first RF frequency and above and passing RF frequencies less than one-fourth of said first RF frequency.

29. A transponder reader according to claim 28 wherein said first RF frequency is 125 KHz.

30. A transponder reader according to claim 29 wherein said RF frequencies less than one-fourth of said first RF frequency are approximately 15.625 KHz and approximately 12.5 KHz.

31. A method for reading an identification signal from an electronic transponder of a radio frequency identification system, said transponder having stored thereon an identification signal including a synchronization portion having a first number of bits, a data portion having a second number of bits, an output format identification portion having a third number of bits and an error detection portion having a fourth number of bits, said method comprising the steps of:

- (1) reading a first number of bits;
- (2) comparing said first number of bits to a known synchronization bit pattern;
- 10 (3) repeating steps (1) and (2) until a known synchronization bit pattern is detected;
- (4) reading bytes of data from the data portion and the output format identification portion one at a time;
- (5) checking parity in each byte read in step (4);
- 15 (6) returning to step (1) if incorrect parity is detected in step (5);
- (7) storing bytes having correct parity;
- (8) repeating steps (4), (5), (6) and (7) until all bytes in said data portion and said output format identification portion have been read;
- (9) reading the error detection byte;
- 20 (10) calculating an error detection value based upon the bytes stored in step (7);
- (11) comparing the error detection byte read in step (9) with the error detection value calculated in step (10) and determining if they are the same;
- (12) returning to step (1) if they are not the same;
- 25 (13) establishing a communications protocol in communicating with a controller, said communications protocol determined by the output format identification portion; and
- (14) transmitting at least a portion of the data portion to the controller.

32. A method according to claim 31 wherein said error detection byte is a cyclic redundancy check value calculated based upon all bits of the data portion and the output format identification portion of the identification signal.

33. A method according to claim 32 wherein said error detection value is a cyclic redundancy check value calculated based upon all bits of the data portion and the output format identification portion of the read bytes.

34. An electronic transponder for use in a radio frequency identification system, said transponder having stored therein an identification signal, comprising:

a first number of bits of memory for storing a synchronization portion of the identification signal;

5 a second number of bits of memory for storing a data portion of the identification signal;

a third number of bits of memory for storing an output format identification portion of the identification signal; and

10 a fourth number of bits of memory for storing an error detection portion of the identification signal.

35. A transponder according to claim 34 wherein said first number is 16 and said bits are set to 0000 0000 0000 0001.

36. A transponder according to claim 35 wherein said data portion and said format identification portion include 13 8-bit bytes each having 7 bits of data and one parity bit.

15 37. A transponder according to claim 36 wherein said parity bits are the least significant bits of each 8-bit byte.

38. A transponder according to claim 36 wherein said parity bits are the most significant bits of each 8-bit byte.

20 39. A transponder according to claim 37 wherein said error detection portion is a 16th 8-bit byte having no parity bits and comprising a CRC error detection value calculated using the 13 8-bit bytes of said data portion and said format identification portion.

40. A transponder according to claim 38 wherein said error detection portion is a 16th 8-bit byte having no parity bits and comprising a CRC error detection value calculated using the 13 8-bit bytes of said data portion and said format identification portion.

25 41. An RF identification system, comprising:

a transponder reader, including,

interrogating means for generating an RF interrogation signal having a first frequency;

receiving means for receiving and demodulating an identification signal

modulated on an RF transponder signal having a second frequency, said second frequency being lower than said first frequency;

a transponder, including,

5 a memory for storing an identification signal, said identification signal having

a synchronization portion, a data portion having stored therein an authorization code number, an output format identification portion having stored therein an output format identifier specifying an output format to be used by said transponder reader, and an error detection portion;

10 a power circuit for powering said transponder in the presence of said RF interrogation signal;

a frequency divider for generating said RF transponder signal;

15 a transmitter for modulating said identification signal onto said RF transponder signal;

an antenna coupled to said transmitter for radiating said RF transponder signal;

a controller for controlling a peripheral device, said controller including,

20 data communications means having a given data communications protocol for communicating with said transponder reader,

a memory for storing access control criteria;

a CPU for comparing said access control criteria with said authorization code number; and

a driver for driving said peripheral device, said CPU activating said driver in response to a comparison of said access control criteria with said authorization code number,

25 said transponder reader communicating with said controller in accordance with said output format specified in said output format identification portion.

1/7

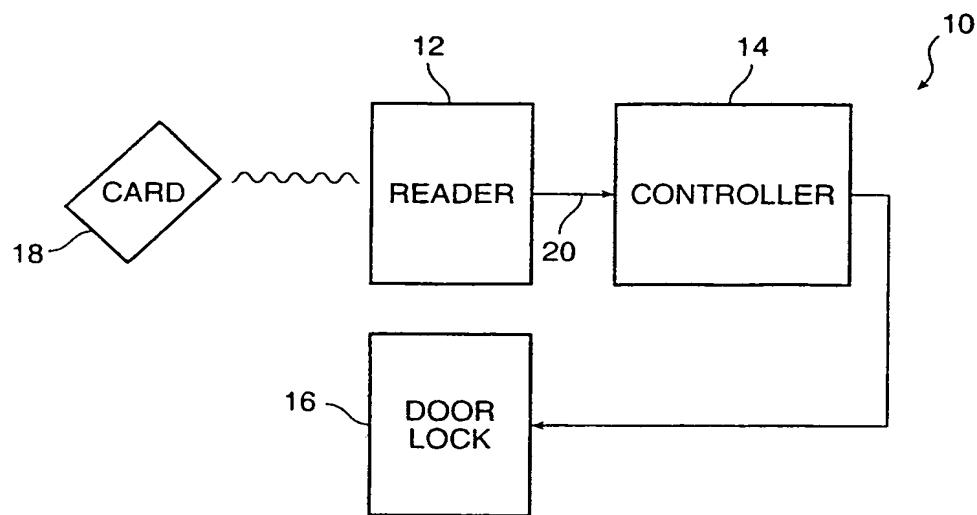


FIG. 1

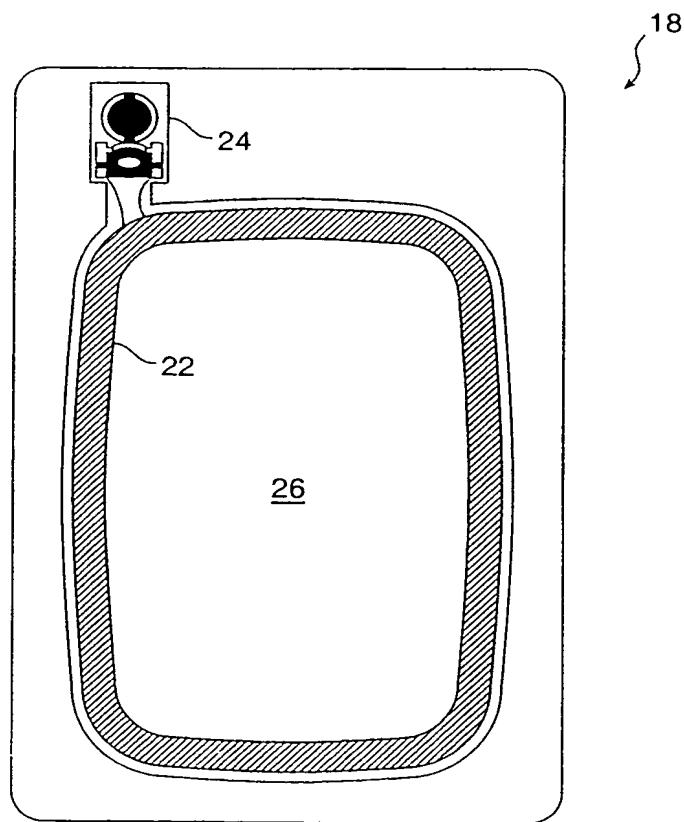


FIG. 2

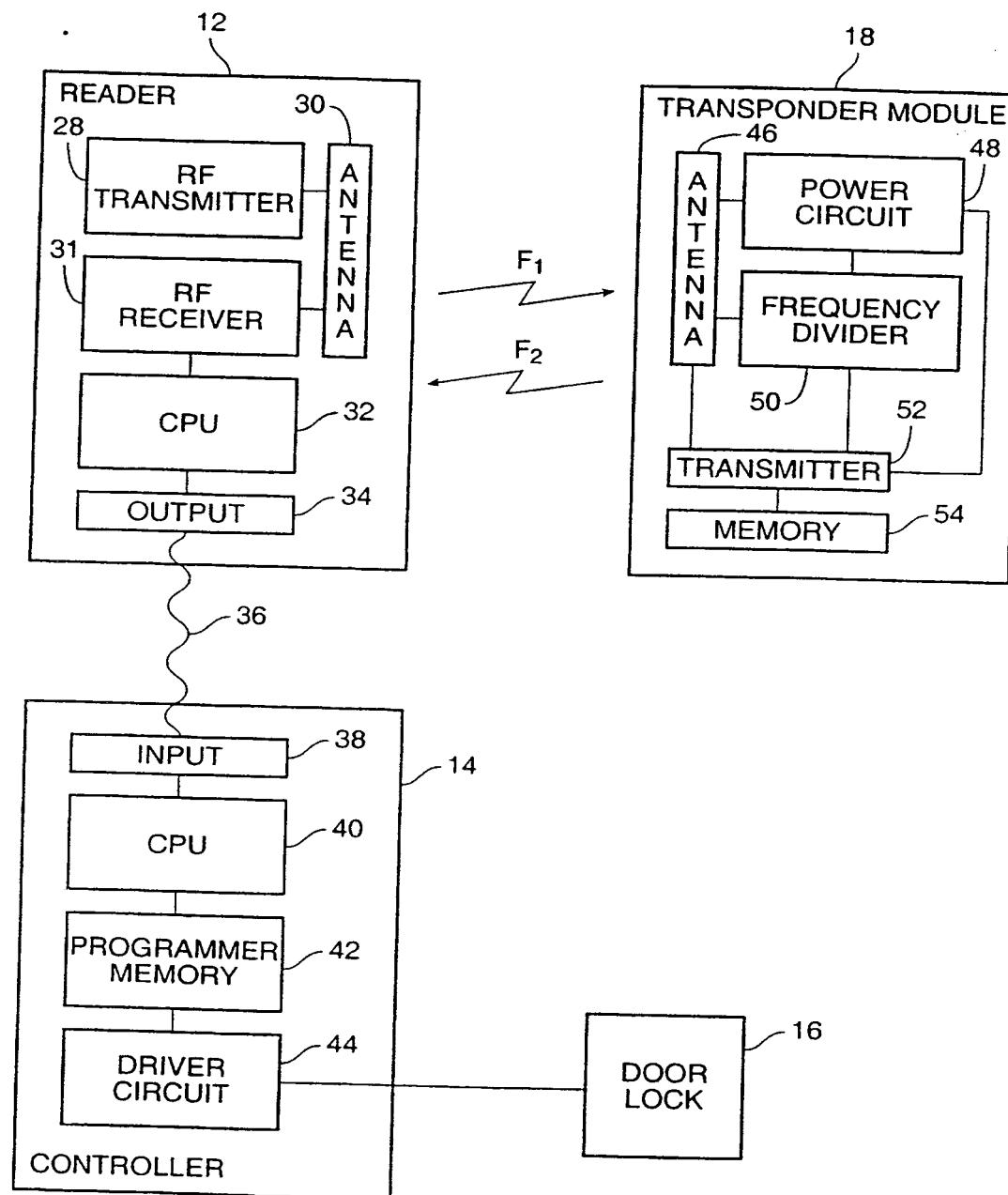


FIG. 3

3/7

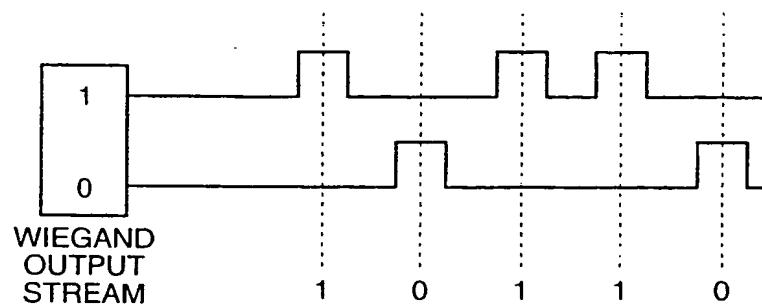


FIG. 4

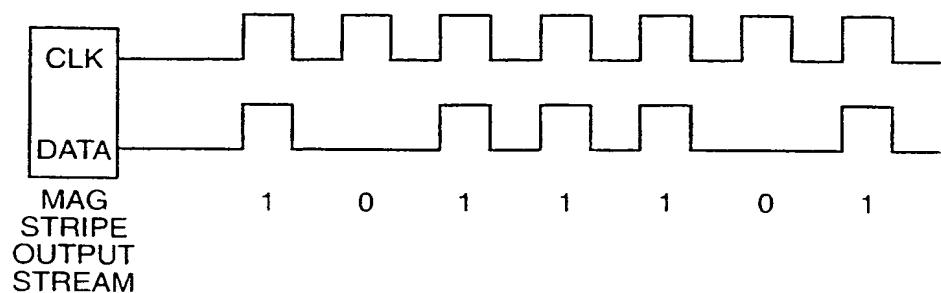


FIG. 5

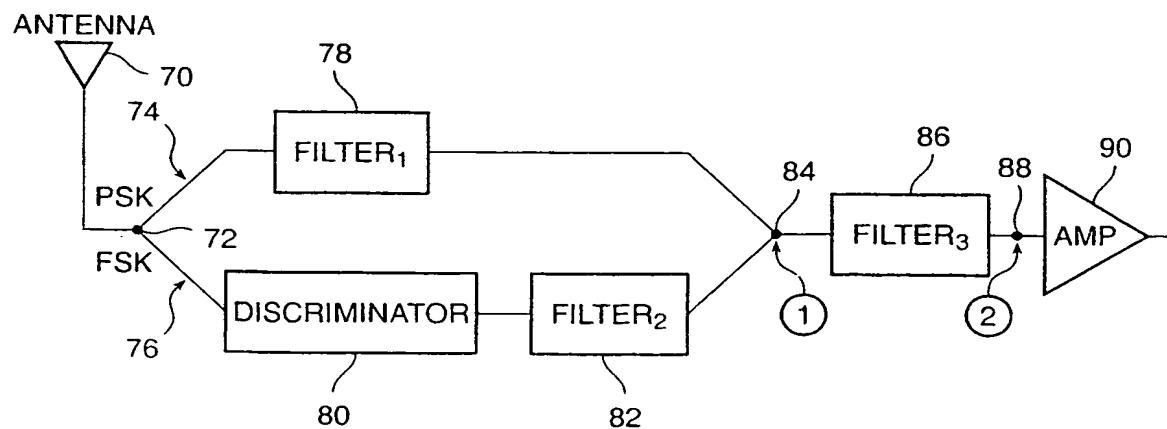


FIG. 6

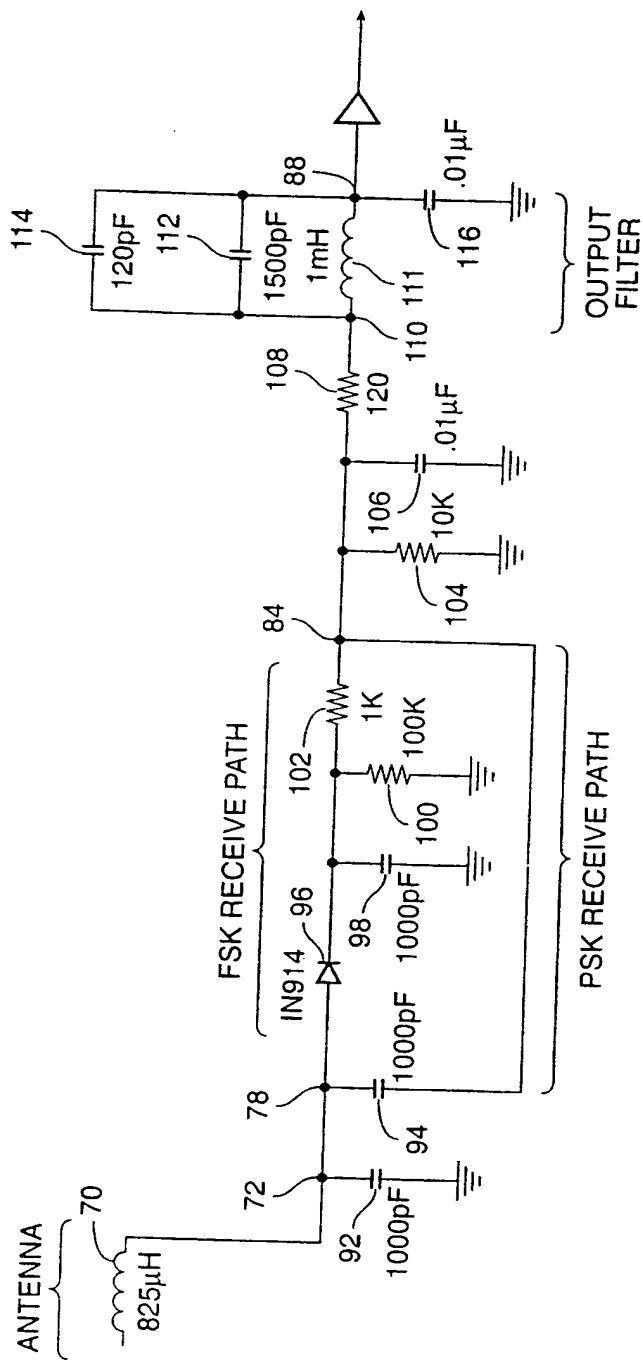


FIG. 7

5/7

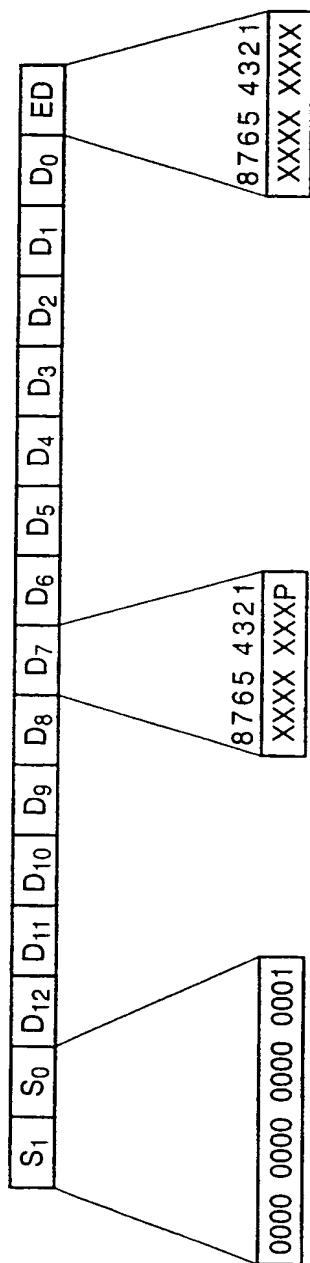


FIG. 8

6/7

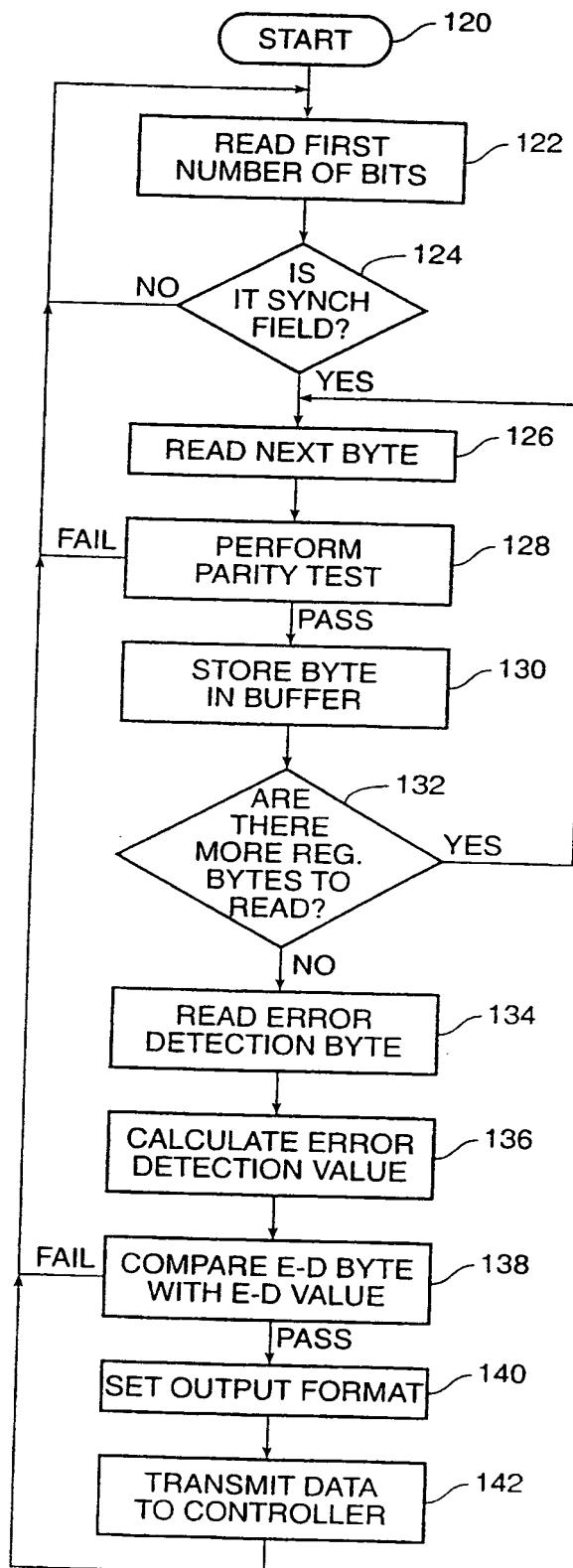


FIG. 9

7/7

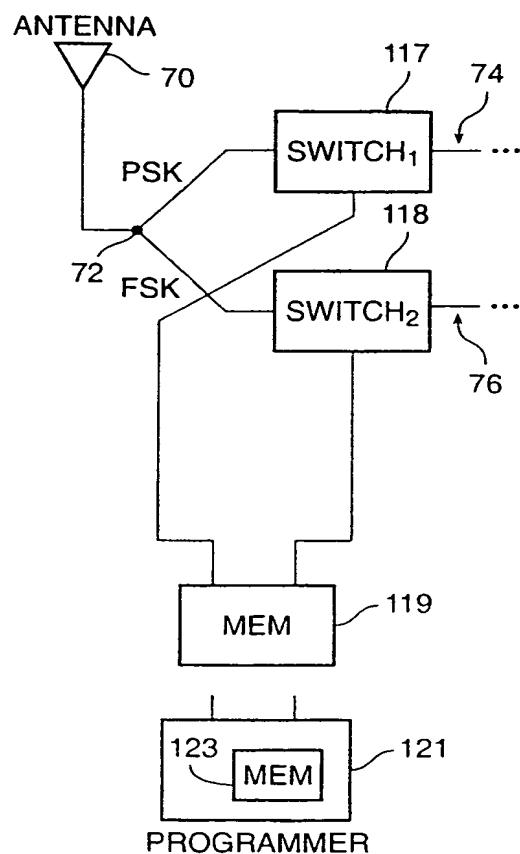


FIG. 10

# INTERNATIONAL SEARCH REPORT

Inten. Application No.  
PCT/US 99/18691

**A. CLASSIFICATION OF SUBJECT MATTER**

IPC 7 G06K7/00 G06K17/00

**B. FIELDS SEARCHED**

Minimum documentation searched (classification system followed by classification symbols)

IPC 7 G01S G07C B61L G06K E05B G07F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

**C. DOCUMENTS CONSIDERED TO BE RELEVANT**

Category	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5 491 471 A (STOBBE ANATOLI) 13 February 1996 (1996-02-13)	1, 10, 19, 20, 27, 34, 41
Y	column 4, line 46 – line 56 column 5, line 37 – line 44; figures 1-4	5-9, 11-15, 17, 25, 31
Y	column 5, line 57 – line 61	5-9
Y	US 4 650 981 A (FOLETTA WAYNE S) 17 March 1987 (1987-03-17) column 6, line 21 – line 26	
Y	US 5 521 602 A (BOND MICHAEL X ET AL) 28 May 1996 (1996-05-28) abstract; figure 1	11, 13-15, 17
A	column 2, line 38 – line 48	26, 28-30
		-/-

Further documents are listed in the continuation of box C.

Patent family members are listed in annex.

\* Special categories of cited documents :

- "A" document defining the general state of the art which is not considered to be of particular relevance
- "E" earlier document but published on or after the International filing date
- "L" document which may throw doubts on priority, claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- "O" document referring to an oral disclosure, use, exhibition or other means
- "P" document published prior to the International filing date but later than the priority date claimed

"T" later document published after the International filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the International search

27 March 2000

Date of mailing of the International search report

03.04.2000

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2  
NL - 2280 HV Rijswijk  
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,  
Fax: (+31-70) 340-3016

Authorized officer

Chiarizia, S

**INTERNATIONAL SEARCH REPORT**

Inte	xnal Application No
PCT/US 99/18691	

**C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT**

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 4 546 241 A (WALTON CHARLES A) 8 October 1985 (1985-10-08) column 2, line 21 - line 30	12
A		16
Y	EP 0 758 777 A (PALOMAR TECHN CORP) 19 February 1997 (1997-02-19) abstract column 2, line 10 - line 21	25
Y	EP 0 569 131 A (MITSUBISHI ELECTRIC CORP) 10 November 1993 (1993-11-10) column 11, line 10 - line 14 column 11, line 26 - line 36	31
X	US 4 963 887 A (HARUYAMA SHINICHI ET AL) 16 October 1990 (1990-10-16)	26
A	column 5, line 51 -column 6, line 24; figure 2	28-30
P, X	WO 98 52168 A (TROESCH PETER ;CRUZ MICHAEL F (US); LU GUIYANG (US); AVID IDENTIFI) 19 November 1998 (1998-11-19) page 5, line 5 - line 13	26

## INTERNATIONAL SEARCH REPORT

International application No.  
PCT/US 99/18691

### Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)

This International Search Report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1.  Claims Nos.: because they relate to subject matter not required to be searched by this Authority, namely:
  
2.  Claims Nos.: because they relate to parts of the International Application that do not comply with the prescribed requirements to such an extent that no meaningful International Search can be carried out, specifically:
  
3.  Claims Nos.: because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

### Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

see additional sheet

1.  As all required additional search fees were timely paid by the applicant, this International Search Report covers all searchable claims.
  
2.  As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment.
  
3.  As only some of the required additional search fees were timely paid by the applicant, this International Search Report covers only those claims for which fees were paid, specifically claims Nos.:
  
4.  No required additional search fees were timely paid by the applicant. Consequently, this International Search Report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

#### Remark on Protest:

The additional search fees were accompanied by the applicant's protest.

No protest accompanied the payment of additional search fees.

FURTHER INFORMATION CONTINUED FROM PCT/IBA/ 210

This International Searching Authority found multiple (groups of) inventions in this international application, as follows:

1. Claims: 1-25, 27 , 31-41

Electronic transponder for use in RF identification system comprising a transmitter for transmitting, and an identifying signal comprising an output format ID portion and parity check portion

2. Claims: 26, 28-30

Transponder reader comprising means for receiving both PSK and FSK modulated signals

A. The special technical features defined in claims 1-25, 27, 31-41 with respect to the document us5491471 are: the features of claim 31 which are not disclosed by said prior art. Namely, the steps of checking parity, solving the objective problem of detecting error in transmission.

B. The special technical features defined in claims 26 and 28 with respect to said prior art. Namely, the means in the reader to deal with PSK as well as FSK, solving the problem of having a reader which is able to deal with transponder of different modulation types.

Thus, there is no common special technical feature to the subjects A and B and these features are neither corresponding features as defined in Rule 13.2 PCT, as they relate to different objectively determined problems and their solutions.

Therefore, the claims do not fulfill the requirements of unity (Rule 13.1 PCT).

**INTERNATIONAL SEARCH REPORT**

Information on patent family members

 International Application No  
**PCT/US 99/18691**

Patent document cited in search report	Publication date	Patent family member(s)		Publication date
US 5491471	A 13-02-1996	DE 4134922 C AT 141430 T CA 2080716 A DE 59206907 D EP 0539763 A		03-12-1992 15-08-1996 24-04-1993 19-09-1996 05-05-1993
US 4650981	A 17-03-1987	NONE		
US 5521602	A 28-05-1996	NONE		
US 4546241	A 08-10-1985	NONE		
EP 0758777	A 19-02-1997	US 5832090 A CA 2182464 A		03-11-1998 11-02-1997
EP 0569131	A 10-11-1993	JP 2842750 B JP 5342435 A DE 69314533 D DE 69314533 T US 5365047 A		06-01-1999 24-12-1993 20-11-1997 19-03-1998 15-11-1993
US 4963887	A 16-10-1990	JP 2064491 A JP 2612190 B CA 1336724 A DE 3928561 A FR 2636187 A GB 2224182 A,B		05-03-1990 21-05-1997 15-08-1995 08-03-1990 09-03-1990 25-04-1990
WO 9852168	A 19-11-1998	AU 7577698 A		08-12-1998